MODELO PARA EL INTERCAMBIO SEGURO DE INFORMACIÓN EN LAS ORGANIZACIONES

DIEGO ALBERTO RICO ROMÁN

UNIVERSIDAD AUTONOMA DE BUCARAMANGA
FACULTAD DE INGENIERIA DE SISTEMAS
GRUPO DE INVESTIGACIÓN PRISMA
LINEA DE INVESTIGACIÓN: GESTION DEL CONOCIMIENTO
BUCARAMANGA
2014

MODELO PARA EL INTERCAMBIO SEGURO EN LAS ORGANIZACIONES

DIEGO ALBERTO RICO ROMÁN

Trabajo de tesis presentado para obtener el título de:
Ingeniero de Sistemas

Director: Msc Freddy Méndez Ortiz

UNIVERSIDAD AUTONOMA DE BUCARAMANGA
FACULTAD DE INGENIERIA DE SISTEMAS
GRUPO DE INVESTIGACIÓN PRISMA
LINEA DE INVESTIGACIÓN: GESTION DEL CONOCIMIENTO
BUCARAMANGA
2014

Nota de aceptación

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bucaramanga 5 de julio de 2014

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

CRIPTOGRAFÍA: Conjunto de técnicas que se utilizan con fines de brindar seguridad a las comunicaciones, a la información y a las entidades que se comunican.

CRIPTOGRAFIA SIMETRICA: Método criptográfico en cual utiliza la misma clave para cifrar y descifrar mensajes.

CRIPTOGRAFIA ASIMETRICA: Método criptográfico el cual utiliza una clave diferente para cifrar y descifrar mensajes a través de una pareja de claves, en donde se usa una clave para cifrar y la otra para descifrar.

CIFRADO: Procedimiento que utiliza un algoritmo con cierta clave la cual transforma un mensaje de forma que no sea comprensible o se dificulte el proceso de comprensión a toda persona que no posea la clave correspondiente.

DESCIFRADO: Procedimiento inverso al cifrado en donde toda persona con la clave adecuada puede tener acceso a un mensaje que se encontraba previamente cifrado

RESUMEN

En la actualidad, las organizaciones manejan diferentes tipos de documentos para comunicarse con los demás empleados, para hacer memorandos, para administrar la información pertinente a la organización entre otros usos.

Aunque se realizan actividades para la reutilización del papel consumido, como el reciclaje, por el cual, una buena parte del papel producido es reutilizado, no es reducido en su totalidad.[1]

Por otro lado debido al avance tecnológico que se presenta actualmente, una empresa u organización puede hacer uso de esta para lograr una disminución en su consumo de papel utilizado dentro de sus actividades diarias, además logrando una gestión más sencilla de su información.

Un modelo tecnológico que utilice técnicas de criptografía que además permita determinar la manera en que realice el proceso de intercambio de información, en donde se estudian las diferentes técnicas y algoritmos basados en criptografías para definir un modelo tecnológico.

Utilizando el modelo tecnológico como base, se pudo realizar un prototipo de un sistema de intercambio seguro de información el cual permite enviar documentos de manera segura a otros usuarios garantizando la identidad del usuario emisor y logrando una mayor seguridad al usuario receptor del mensaje. Por lo tanto, el modelo correctamente aplicado permite servir como una alternativa viable para el intercambio seguro de información.

Palabras clave: Modelo, criptografía, seguridad, BPMN, RSA

[1] ANDI Consumo aparente Primer semestre de 2012 [En línea] <http://www.andi.com.co/Archivos/file/Consumo%20aparente%20primer%20semestre%20%202012.xls>

INTRODUCCIÓN

En las organizaciones se manejan un gran número de documentos impresos que se entregan a sus empleados, por lo cual, la cantidad de papel invertido en la impresión de estos documentos es elevada, especialmente en el caso de organizaciones con un alto número de empleados.

Debido al avance tecnológico que se presenta actualmente, una empresa u organización puede hacer uso de esta para lograr una disminución en su consumo de papel utilizado dentro de sus actividades diarias, además logrando una gestión más sencilla de su información.

A día de hoy existen diferentes alternativas para la reducción del consumo de papel utilizando tecnología entre estas se encuentran la utilización de correo electrónico, utilización de herramientas alternativas de comunicación como los sistemas de mensajería instantánea y el uso de gestores documentales, los cuales permiten administrar y enviar documentos de manera más organizada, a pesar de esto, estas alternativas no ofrecen medidas de seguridad en lo que se refiere a la información enviada.

La criptografía posee un conjunto de técnicas que permiten brindar seguridad a la información, a través del uso de algoritmos que permiten crear claves únicas, permiten proteger la información a través del proceso de cifrado en donde se utiliza la clave creada para generar protección a la información dejándola protegida al acceso de terceros y en donde para poder ser vista, se utiliza el proceso inverso conocido como descifrado el cual utiliza la clave creada para retornar la información cifrada a su estado original, a pesar de esto no existen muchas aplicaciones ampliamente difundidas que utilicen técnicas de criptografía para el intercambio de documentos.

Por eso la implementación de un sistema que permita realizar el mismo manejo de información utilizando técnicas de criptografía de forma que la información a manejar sea más confiable y segura podría ser una alternativa para lograr reducir el consumo de papel en una organización. En esta solución donde se planea a través de la definición de un modelo tecnológico que permita definir un proceso a realizar dentro de las organizaciones con fines de proveer un servicio de intercambio seguro de información entre dos usuarios de manera en que esta información no pueda ser interceptada por usuarios no autorizados.

Para lograr lo anterior mencionado se tiene planeado realizar a través de las siguientes actividades: La caracterización de las diferentes alternativas tecnológicas que pueden ser utilizadas para la solución y elegir la más apropiada para el caso de estudio, el diseño de un modelo que permita ofrecer una solución al problema del elevado consumo de papel dentro del proceso de memorandos de gestión humana, que permita además gestionar la información de manera segura y confiable, La implementación de un prototipo funcional basado en el modelo que permita validar la solución propuesta al problema, la validación del prototipo mediante la aplicación de pruebas controladas que permitan verificar el correcto funcionamiento del prototipo.

Este modelo tecnológico permitirá definir un procedimiento a realizar explicado a través de BPMN que permitirá explicar el proceso de intercambio de información entre dos usuarios explicando también la interacción de estos usuarios con el sistema encargado de realizar el manejo y envío de información segura entre dos usuarios, este sistema generado a base del modelo tecnológico se definirá a nivel de aplicaciones a utilizar para que este funcione, también se definirá a nivel de hardware, en donde se especificará el hardware necesario para que la aplicación se pueda utilizar

1. ANALISIS Y PRUEBAS DE TECNICAS DE CRIPTOGRAFIA

Existen diferentes algoritmos de criptografía utilizados para la generación de llaves, las cuales son utilizadas para el proceso de cifrado y descifrado de información, estos algoritmos se pueden clasificar en dos maneras distintas: en la manera en la que el algoritmo cifra su información y en la utilización de la misma llave para el descifrado de información o el uso de una llave diferente para el cifrado y descifrado de información, a continuación se explicarán cada una de estas características junto con los algoritmos criptográficos que posean dichas características, esto es necesario para la elección del algoritmo de cifrado más efectivo

Cifrado en bloque

Como su nombre lo indica, los algoritmos criptográficos que serán explicados a continuación realizan el cifrado de información utilizando múltiples bloques de bits, dándoles así una rápida velocidad de cifrado

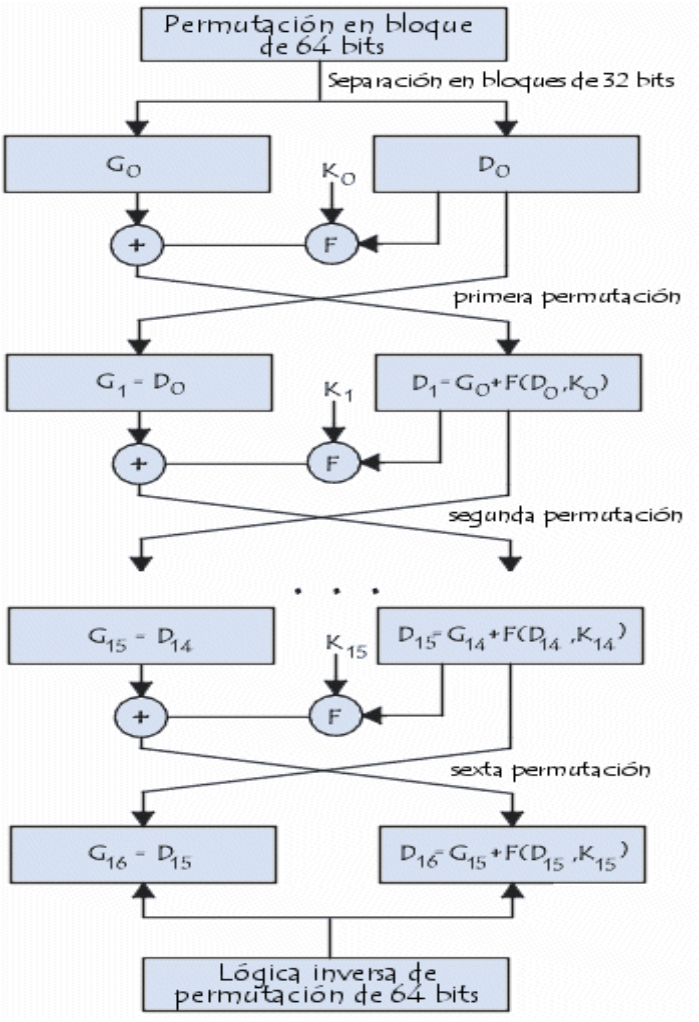
DES

El estándar de encripción de datos (DES) es uno de los algoritmos más antiguos y fue difundido ampliamente durante los años setenta este algoritmo posee las siguientes características:

- El texto original se codifica en bloques de 64 bits, clave de 56 bits y 19 etapas diferentes.
- El descifrado se realiza con la misma clave y los pasos inversos.
- El inconveniente es que puede ser descifrado probando todas las combinaciones posibles, cosa que queda solucionada con Doble DES (ejecuta el DES 2 veces con 3 claves distintas) y el Triple Des (2 claves y 3 etapas).

El algoritmo DES consiste en la división de los bloques de 64 bits en dos bloques de 32 en donde estos dos bloques divididos realizan un proceso múltiple de permutación en donde estos bloques se alteran como resultado de cada una de las permutaciones realizadas en cada permutación se aplica una función la cual genera el cambio respectivo a cada uno de los bloques, para el proceso de descifrado, se realiza el proceso inverso, es decir, el algoritmo sigue el procedimiento de abajo hacia arriba como se puede ver en la figura 1 comenzando desde la sexta permutación regresando a través de las seis permutaciones y luego volviendo a unir los dos bloques de 32 bits al bloque original de 64 bits.

Figura 1. Proceso de cifrado del algoritmo DES



Fuente: Kioskea Introducción al cifrado mediante DES

Este algoritmo no es muy utilizado actualmente debido a su cifrado de pequeño tamaño que a pesar de que se puede realizar un triple cifrado el tamaño de su cifrado sigue siendo relativamente pequeño respecto a otros algoritmos.

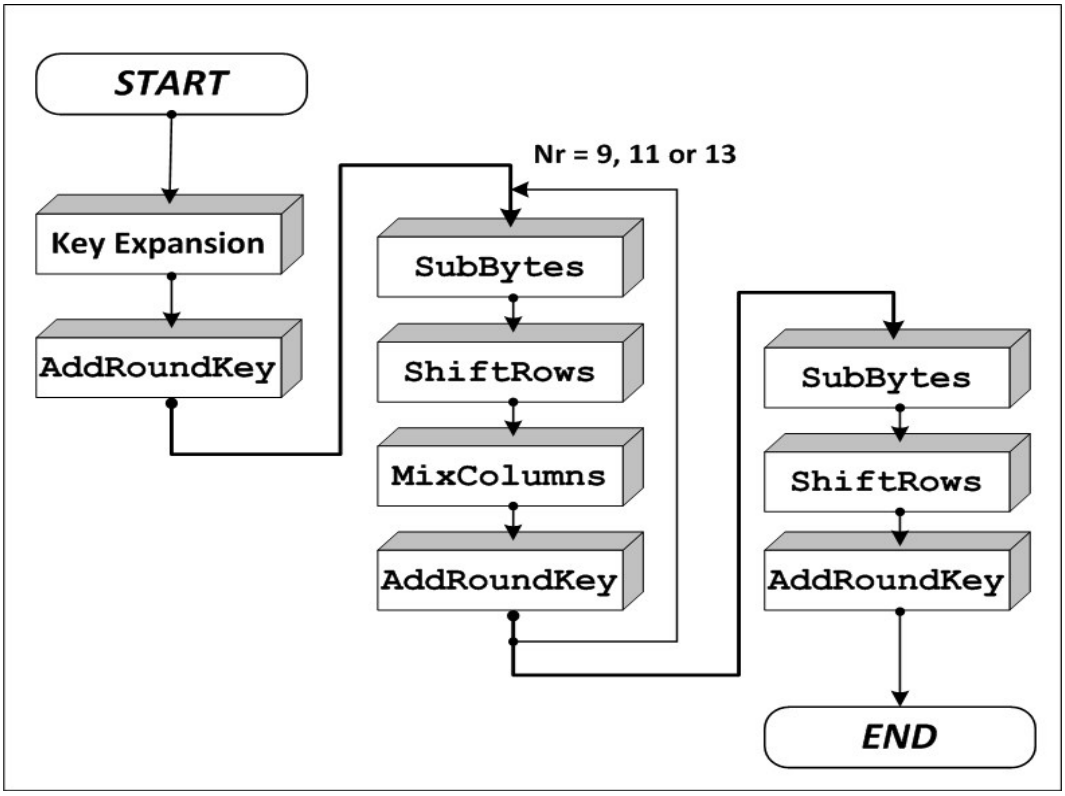
AES

El estándar de encripción avanzado (AES) es un algoritmo de cifrado por bloques, este algoritmo de cifrado es utilizado como estándar de encripción por parte del gobierno de estados unidos, el tamaño de bloque del algoritmo AES posee un tamaño fijo de 128 bits en donde sus llaves pueden tener hasta un tamaño de 256 bits.

AES se maneja una matriz de 4x4 bytes en donde su proceso de encripción está compuesto de 4 fases principales las cuales manejan las llaves a través de la matriz generada para completar el proceso de cifrado, las cuatro fases principales se mencionan a continuación:

- AddRoundKey: En esta fase cada uno de los bytes que se enuentra dentro de la matriz 4x4 del algoritmo AES se combina con la clave la cual se denomina de ronda o “round” en ingles la cual proviene de la llaves AES a utilizar
- SubBytes: En esta fase se realiza una sustitución de bytes utilizando una matriz de búsqueda que viene definida por el algoritmo.
- ShiftRows: En este operación se realiza una transposición de cada una de las filas de la matriz 4x4 en manera cíclica en donde cada una de las filas de la matriz rota de manera diferente. En cada fila
- MixColumns: Esta realiza una mezcla de columnas dentro de la matriz 4x4 del algoritmo AES usando una transformación lineal

Figura 2. Gráfico de flujo que explica el proceso del algoritmo AES



Fuente: AMD Bulk encryption on GPUs

RSA

El algoritmo RSA es uno de los algoritmos más utilizados actualmente debido a la alta complejidad computacional que tiene poder descifrar un mensaje cifrado mediante este algoritmo

Su algoritmo se basa en la dificultad de factorizar números grandes por parte de los ordenadores, al factorizar grandes número dificultará el proceso para descifrar su mensaje, el algoritmo es el siguiente:

- Dividimos el texto normal en bloques P, que cumplen que 0<P<n
- Para cifrar un mensaje P calculamos C = p^e(mod n).
- Para descifrar C calculamos P = C^d (mod n).

Cabe destacar que la dificultad de este algoritmo radica en el calcula de P el cual puede tomar un tamaño bastante grande, dándole un tiempo de cálculo computacional bastante grande para poder calcular un solo valor de P cunado este algoritmo puede tener una gran rango de valores para P

A pesar de los tres algoritmos mencionados anteriormente son algoritmos de cifrado en bloques es necesario destacar que los algoritmos DES y AES utilizan la misma llave para cifrar y descifrar mensajes mientras que el algoritmo RSA utiliza una llave distinta para cifrar y otra para descifrar de manera de que este conjunto de llaves es único y cada llave es complementaría de la otra.[2]

Cifrado de flujo

Es un cifrado el cual se realiza bit por bit, algunos algoritmos que utilizan cifrado de flujo son los siguientes:

- RC4

  Es un algoritmo de cifrado flujo utilizado frecuentemente para lograr un tráfico más seguro en internet, este algoritmo no es muy usado actualmente siendo reemplazado por otros algoritmos de cifrado como el algoritmo AES.

  Este algoritmo en términos sencillos funciona a través de la generación de una matriz la cual posee un valor especial para cada bit en donde se utiliza un algoritmo generador aleatorio para transformar cada bit de información del mensaje a un equivalente cifrado utilizando la matriz generada como base para la generación de la salida cifrada de la información.

[2] PENALVA, Cristóbal. Seguridad:Criptografía [En línea] <http://www.uv.es/montanan/redes/trabajos/criptografia.doc>

- SEAL

  SEAL es un algoritmo de cifrado de flujo el cual se calculan los valores a para un conjuntos cuyos datos vienen a partir de la llave utilizada, Su funcionamiento se basa en un proceso inicial en el que se calculan los valores para unas tablas a partir de la llave, de forma que el cifrado propiamente dicho puede llevarse a cabo de una manera realmente rápida. Una característica muy útil de este algoritmo es que no se basa en un sistema lineal de generación, sino que define una familia de funciones pseudo-aleatorias, de tal forma que se puede calcular cualquier porción de la secuencia suministrando únicamente un número entero n de 32 bits.[3]

  SEAL se basa en el empleo del algoritmo SHA para generar las tablas que usa internamente.

La otra manera de clasificar los algoritmos criptográficos es por el uso de luna misma llave o el uso de una llave diferente para el proceso de cifrado y descifrado de información esto se conoce como criptografía simétrica y asimétrica:

Cifrado con clave secreta o Criptografía simétrica En estos sistemas existirá una única clave (secreta) que deben compartir emisor y receptor. Con la misma clave se cifra y se descifra por lo que la seguridad reside sólo en mantener dicha clave en secreto.

La confidencialidad y la integridad se lograrán si se protegen las claves en el cifrado y en el descifrado. Es decir, se obtienen simultáneamente si se protege la clave secreta.

Cifrado con clave pública o Criptografía asimétrica En estos sistemas cada usuario crea un par de claves, una privada para descifrar y otra pública para cifrar, inversas dentro de un cuerpo finito. Lo que se cifra en emisión con una

[3] BRAVO, Silvana. Estudio comparativo de los algoritmos de cifrado de flujo RC4 A5 y SEAL [En línea] <http://delta.cs.cinvestav.mx/~francisco/arith/Flujo.pdf>

clave, se descifra en recepción con la clave inversa. La seguridad del sistema reside en la dificultad computacional de descubrir la clave privada a partir de la pública.

1.1 EL CONTROL DE INTEGRIDAD

Además en la criptografía de clave pública se ejerce también un control de la integridad cuya función es asegurarnos de que el mensaje recibido fue el enviado por la otra parte y no uno manipulado, para cumplir con este objetivo se utilizan funciones de dispersión unidireccional (o hash).

La función de dispersión llamada compendio de mensaje, tiene 3 propiedades importantes:[4]

1. Dado un mensaje P, es fácil calcular el compendio del mensaje MD (P).
2. Dado un compendio MD (P), es computacionalmente imposible encontrar P, es decir no tiene inversa.
3. No se pueden generar dos mensajes que tengan el mismo compendio, a menos que sean el mismo mensaje.

Y gracias esto, es posible lograr la autenticación un mensaje, además de saber que un mensaje no ha sido manipulado por otra persona que haya interceptado el mensaje

[4] PENALVA, Cristóbal. Seguridad:Criptografía. [En línea] <http://www.uv.es/montanan/redes/trabajos/criptografia.doc>

1.2 EL NO REPUDIO Y FIRMA DIGITAL

El no repudio, consiste en que el receptor puede saber a ciencia cierta de quien es el mensaje y esto lo podemos conseguir mediante la firma digital, al ser esta única, como si fuera una firma normal en un papel, tenemos como un acuse o un recibo, que demuestra quién ha enviado el mensaje.

Esto es un añadido a todo lo visto anteriormente que incluye más seguridad a la transmisión de mensajes entre los usuarios. Además la firma digital puede ser utilizada al igual que el hash tanto en los sistemas de clave pública como en los de clave privada. Por este motivo es muy utilizada en documentos legales y financieros.

Requisitos de la firma digital:

a) Debe ser fácil de generar.
b) Será irrevocable, no rechazable por su propietario.
c) Será única, sólo posible de generar por su propietario.
d) Será fácil de autenticar o reconocer por su propietario y los usuarios receptores.
e) Debe depender del mensaje y del autor[5]

1.3 TIPOS DE FIRMA DIGITAL

Firma digital básica La firma digital básica es un conjunto de datos recogidos electrónicamente que formalmente identifican al autor y se incorporan al propio documento. El problema de este sistema es que no se puede saber a ciencia cierta si el documento ha sido creado por la persona que lo firma o si

[5] PENALVA, Cristóbal. "Seguridad:Criptografía". [En línea]: <http://www.uv.es/montanan/redes/trabajos/criptografia.doc>

verdaderamente lo ha firmado él y no una tercera persona que ha suplantado su identidad.

Por lo tanto este tipo de firma es muy básica y puede presentarse el caso de que esta sea alterada, quitándole seguridad al mensaje.[6]

Firma digital avanzada La firma digital avanzada permite la identificación del emisor del mensaje ya que está vinculada de manera única al que firma el documento y a los datos que incorpora, ya que es el signatario quien únicamente posee el control exclusivo de estas claves. Además permite saber si estos datos han sido modificados posteriormente o en su transcurso. A esta firma la ley le otorga plena eficacia jurídica y valor probatorio en juicio.

La firma digital avanzada, a través de su sistema de criptografía asimétrica o de clave pública y privada, no solo garantiza la autenticidad del documento electrónico, sino que también garantiza su integridad, confidencialidad y el no repudio de su transmisión o recepción.

Esto quiere decir que la firma digital avanzada garantiza que el emisor del documento es quien dice ser y además certifica que el documento no ha sido modificado después del momento de la firma. Del mismo modo, asegura que la información cifrada solo será accesible al destinatario de la misma. Con la característica del no repudio se pretende que ni el emisor pueda negar haber enviado el documento, ni que el receptor pueda negar haberlo recibido.[7]

[6] EROSKI CONSUMER. La firma electrónica [En línea] <http://www.consumer.es/web/es/tecnologia/internet/2005/02/13/117226.php#>

[7] MODELO FACTURA Firma digital avanzada [En línea] <http://www.modelofactura.net/firma-digital-avanzada.html>

Firma digital reconocida Si existe un tipo de firma digital capaz de alcanzar todas las medidas de seguridad que ofrece la firma manuscrita, esa es la firma digital reconocida. Este tipo de firma es la que le ofrece al emisor y al receptor la mayor seguridad posible.

Una firma digital reconocida es una firma avanzada, pero basada en un certificado reconocido y además generada a partir de un dispositivo seguro de creación. El certificado reconocido, que se consigue a través de un prestador de servicios de certificación, verifica presencialmente la identidad del autor de la firma.

Al igual que la firma digital avanzada, la firma digital reconocida se basa en la criptografía asimétrica o un sistema de clave pública y privada. De esta forma obtiene los mismos elementos de seguridad, tales como autenticidad, integridad, confidencialidad y no repudio.

Gracias a todos estos mecanismos de seguridad, la firma digital reconocida tendrá el mismo valor que la firma manuscrita de un documento en papel.
Como complemento, en la práctica a aparecen otra serie de tipos relativos a la comprobación de validez de los certificados o la inclusión de marcas de tiempo.[8]

Firma con sello temporal o fechado Firma electrónica a la que se le ha añadido un sello de tiempo. El sellado de tiempo (o *timestamping*) es un mecanismo que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. La autoridad de sellado de tiempo (TSA, del inglés *Time Stamping Authority*) actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

[8] MODELO FACTURA. Firma Digital Reconocida. [En línea]
<http://www.modelofactura.net/firma-digital-reconocida.html>

Firma validada o completa: Firma electrónica fechada a la que se le ha añadido información sobre la validez del certificado procedente de una consulta de CRL u OCSP realizada a la Autoridad de Validación.

Firma longeva o de larga duración: Consiste en una firma electrónica validada dotada de validez a lo largo del tiempo. Esto se consigue incluyendo en la firma todos los certificados de la cadena de confianza y el resultado de la comprobación de validez de los mismos en el momento en el que se realizó la firma, así como por ejemplo al ir refirmando y actualizando los sellos de tiempo de forma regular. Este proceso de refirmado se utiliza para garantizar que unos datos que fueron firmados con un algoritmo que era válido en su día, pero inseguros actualmente debido a la evolución tecnológica, no pierdan valor ya que se han ido refirmando siempre con algoritmos criptográficos seguros en cada momento.[9]

1.4 CERTIFICADOS ELECTRÓNICOS

Los certificados son documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad. Permiten verificar que una clave pública específica pertenece efectivamente a un individuo o entidad.

Los certificados, de esta forma, ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona. En algunos casos, puede ser necesario crear una cadena de certificados, donde cada uno certifica el anterior, para que de esta forma las partes involucradas confíen en la entidad en cuestión.

Un certificado puede utilizarse para identificarse en cualquier tipo de transacción o comunicación electrónica. Permite garantizar que un mensaje emitido ha sido enviado por el titular del certificado y que no ha sufrido ninguna alteración.

[9] ZONATIC Sistemas actuales de autentificación y firma [En línea] <http://zonatic.usatudni.es/es/aprendizaje/aprende-sobre-el-dnie/57-aspectos-tecnicos/208-sistemas-actuales-de-autenticacion-y-firma.html>

Los certificados digitales se almacenan a través de un PKCS#12 o P12.
Este es un archivo que contiene la información definida por el estándar PKCS#12 (Personal Information Exchange Syntax Standard) y en el formato que éste también define.

Concretamente, estos ficheros contienen un certificado digital, junto con la clave privada correspondiente y los certificados de todas las autoridades de certificación hasta la que es la raíz (o, como se le denomina, la cadena de certificación). Los ficheros están cifrados con una contraseña.

Adicionalmente los certificados se pueden guardar en: tarjetas inteligentes o dispositivos token estos dispositivos son para el manejo específico de certificados digitales.

También se pueden almacenar en dispositivos de almacenamiento como Discos magnéticos, memorias USB para almacenar el certificado digital en este tipo de dispositivos debe ser generado en formato P12.
En Colombia la única certificadora abierta que existe es La Sociedad Cameral de Certificación Digital Certicámara S.A., o simplemente Certicámara, es una sociedad anónima constituida por las cámaras de comercio del país con el objetivo de prestar los servicios de certificación digital que se regulan por la ley 527 de 1.999, el Decreto 1747 de 2.000[10] y las demás normas que las complementen, modifiquen o reemplacen. [11]

[10] ALCADIA DE BOGOTA Decreto 1747 de 2000 [En línea] <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277>

[11] CONTRALORÍA DE BOGOTÁ. Conceptos de Firma (Certificado) Digital . [En línea] <http://sivicof.contraloriabogota.gov.co/stormUser/Documentos/Conceptos%20de%20Firma%20Digital.pdf>

1.4.1 Creación de certificados digitales propios Además de la creación de certificados digitales por parte de una autoridad certificadora como Certicámara, también existe la posibilidad de crear un certificado digital en donde el mismo usuario puede crear su propio certificado. El cuál puede resultar útil cuando al usuario al cual le enviamos información confía abiertamente en que nosotros somos el verdadero usuario, crear un certificado propio no tiene ningún costo.

Una de las herramientas posibles para la creación de certificados digitales propios es a través del uso de la herramienta OpenSSL el cuál es un paquete que permite agregar elementos de encriptación a nuestro sistema y poder crear certificados digitales que pueden aplicarse dentro de un servidor.

OpenSSL permite crear sus conjuntos de llaves que se utilizan para poder firmar el certificado, esto con el fin de proporcionar seguridad a través de un algoritmo de cifrado como el RSA junto a un algoritmo hash como SHA
Al momento de la creación del certificado digital se debe llenar con la información pertinente que se solicita para poder hacer una identificación del individuo que este creando el certificado.

Además el certificado puede firmarse e ir con un algoritmo de cifrado el cual contiene una llave pública y una privada para dar protección al archivo, y asegurar además de que el documento no haya sido modificado.

Para estudiar el uso de certificados digitales se estudió el proceso que maneja la DIAN con sus certificados digitales, dentro de este proceso, la DIAN maneja un proceso de registro de datos del solicitante del certificado, donde como resultado se obtendrá un certificado digital el cuál identificará al usuario al momento de hacer algún proceso con la DIAN, además para el acceso al certificado se incluye una contraseña, así de esta manera ayudará a evitar que otra persona diferente al dueño del certificado pueda utilizarlo, en donde el

usuario que creó el certificado podrá identificarse al momento de hacer algún proceso en línea solicitado por la DIAN.[12]

1.5 PRUEBA DE LAS DIFERENTES TÉCNICAS DE CRIPTOGRAFÍA

Se realizó una un análisis para encontrar una solución idónea para aplicar al problema definido inicialmente en donde se comparó inicialmente la alternativa de firmas digitales y la opción del uso de certificados digitales.

De manera inicial, las firmas digitales, existen diferentes servicios a nivel online que permiten crear su propia firma digital, además pueden dar autentificación al usuario debido a que una firma digital puede vincularse al usuario, la desventaja que posee esta alternativa es la poca manipulación que permiten estas firma brindadas por entidades externas, esto es debido a que las firmas son obtenidas por autoridades o servicios los cuales brindan la firma ya hecha la cual no permite una alteración a menos de que se contacte con la autoridad que le brindó la firma, no se ofrece la posibilidad de que el usuario cree su propia firma digital por medios propios, debido a esto, no es una opción muy viable para el proyecto a realizar.

Analizando la alternativa de la implementación de los certificados digitales, existen dos alternativas para conseguir un certificado digital, la primera es consiguiéndolo mediante una autoridad certificadora, esta autoridad asegura, que el certificado corresponde a la persona quien dice ser, en donde en el caso de Colombia Certicámara es la autoridad responsable de brindar los certificados digitales, estos certificados brindados por la autoridad certificadora tienen un precio. La otra alternativa es a través de la creación certificados digitales propios, en donde el usuario que los crea es la propia autoridad certificadora, la desventaja de esto, es que entidades externas pueden no confiar en los

[12] DIAN “Mecanismo Digital”. [En línea] <http://www.dian.gov.co/descargas/cartillas/Dian-guiaMecanismosDigitales-V1-04_130208.pdf>

certificados creados por un individuo ajeno a una autoridad certificadora, pero en casos en donde los individuos confíen en nuestros certificados, es una buena alternativa para aplicar debido a que esto no tiene ningún costo.

La desventaja que poseen estos certificados propios del uso de certificados digitales para cifrar documentos para su protección, es que normalmente el tamaño tolerado que permite un certificado digital para su cifrado es relativamente pequeño, por lo que no es muy conveniente utilizarlo para estos fines.

Por otro lado se analizó el uso del conjunto de llaves basada en criptografía asimétrica para el cifrado y descifrado de documentos, en donde permitió el cifrado de documentos de tamaño considerable, en este cifrado, se utilizó la clave pública para cifrar el documento, y se descifra utilizando la clave privada del conjunto de llaves, al intentar utilizar una clave privada diferente a la creada junto con la llave pública, no permitirá descifrar el documento, aportando de esta manera seguridad a los archivos para que de estas manera no sean modificados por otra personas que no posean el conjunto de claves necesarios para descifrar el archivo cifrado.

En la siguiente tabla la cual será mostrada a continuación se mostrará la comparación de cada una de las técnicas de protección de información estudiadas, en donde se mostrará las ventajas y desventajas que poseen cada una de estas técnicas estudiadas.

Tabla 1. Tabla comparativa técnicas de protección de información, basadas en criptografía

Técnica	Ventajas	Desventajas
Firmas Digitales	Permite identificar fácilmente a un usuario	Las firmas son creadas por una autoridad certificadora, por lo tanto no son gratuitas
	Permite saber si un documento ha sido modificado gracias al control de integridad	No existen de momento herramientas conocidas para la creación de firmas digitales propias y sin costo
Certificados Digitales	Posee las mismas características de una firma digital	Es principalmente utilizada para el acceso a sitios seguros, y no para la protección de documentos
	Existe la opción de crear certificados digitales propios de forma gratuita	Solo permite el cifrado a documentos pequeños
Llaves criptografía asimétrica	El uso de una llave distinta para el cifrado y descifrado dificulta el acceso al documento protegido por parte de usuarios no autorizados	Su método de utilización puede resultar complejo para personas menos versadas en el área de tecnología
	Es posible crear el conjunto de llaves propias y de forma gratuita	

Fuente: Autor del proyecto

De esta manera, analizando las diferentes técnicas, se optó para este proyecto, la alternativa de la utilización de llaves a través de criptografía asimétrica, esto es debido a que la alternativa de los certificados digitales no es viable debido a que estos son mayormente utilizados para la autentificación de usuarios y no para la firma de documentos.

Como parte de la utilización de llaves de criptografía asimétrica se utilizará el algoritmo RSA, la razón de su uso se sustenta en que es un algoritmo robusto que permite hasta 2048 bits de cifrado, convirtiéndolo en un algoritmo más difícil de descifrar, y por lo tanto, más seguro; Se tendrá también en cuenta una utilización más sencilla del conjunto de llaves, de forma en que no se conviertan en una dificultad de manejo para los usuarios.

2. WORKFLOW

Workflow se refiere al flujo de trabajo a seguir para la consecución de una tarea o trabajo predeterminado. Se define como un sistema de secuencia de tareas de un proceso de negocio. Su definición y control puede ser manual, informatizado o mixto. Organiza y controla tareas, recursos y reglas necesarias para completar el proceso de negocio**.**

La evolución de Workflow consiste en buscar la máxima automatización de los procesos de trabajo y el control total de las diferentes etapas, durante las cuales los documentos, la información o las tareas pasan de un participante a otro, según unas normas o procedimientos previamente definidos.

A lo largo del tiempo, se han ido desarrollando diversas aplicaciones de software, muchas de ellas han evolucionado a partir de sistemas de gestión de imagen, sistemas de gestión de documentos, sistemas de correo electrónico o de bases de datos.[13]

El Workflow permite también definir de forma sencilla como los procesos son realizados de manera que sea fácil de comprender y mantener un buen nivel de detalle, ideal para realizar un modelado para explicar el funcionamiento de un proceso.

2.1 BPMN

Una notación sencilla para realizar los flujos de trabajo o Workflow es a través de la notación BPMN**;** BPMN es un lenguaje formal que permite modelar, simular y, eventualmente, ejecutar procesos de negocios.

[13] PIXELWARE. Workflow: Flujo de trabajo [En línea] <http://www.pixelware.com/workflow-flujo-trabajo.htm>

Su sintaxis está basada en elementos gráficos, pero tales elementos tienen una relación uno a uno con instrucciones en el Lenguaje BPEL, lo cual permite generar código ejecutable BPEL a partir de un modelo BPMN. Fue desarrollado por la organización BPM Initiative, pasando posteriormente a fundirse con los esfuerzos que en paralelo realizaba el OMG.

Con esto hay grandes posibilidades de que BPMN se convierta en el lenguaje estándar acerca de procesos de negocios, tal como UML, bajo el auspicio de la OMG, se ha convertido en el estándar para modelamiento de software.

2.1.1 Elementos BPMN básicos. Cabe recalcar que una de las directrices para el desarrollo de BPMN es crear un mecanismo simple para diagramar flujos de proceso y que a su vez maneje la complejidad inherente a los procesos del negocio, o dentro de este caso el modelo tecnológico a plantear. El acercamiento tomado para manejar estos dos requisitos que estaban en conflicto fue el organizar los aspectos gráficos de la notación en categorías específicas.

El sitio web de la aplicación Bizagi, aplicación que será utilizada dentro de este proyecto para la definición de modelos en BPMN explica el funcionamiento de sus elementos básicos los cuales serán explicados a continuación para una mejor comprensión del modelo en BPMN que será mostrado más adelante.
Bizagi categoriza sus elementos en cuatro categorías básicas las cuales son explicadas a continuación: [14]

[14] BIZAGI BPMN (Bussiness Process Model and Notation) [En línea] <http://wiki.bizagi.com/es/index.php?title=BPMN>

Tabla 2. Elementos básicos de BPMN

ELEMENTO	DEFINICIÓN	VERSION ANTERIOR	NOMBRE BPMN
Elementos de Flujo (Flow Objects)	Los elementos de flujo son los principales elementos gráficos que definen el comportamiento de los procesos.	Eventos	Events
		Actividades	Activities
		Decisión	Gateways
Conectores (Connecting Objects)	Los objetos del flujo se conectan entre ellos a través de los conectores para crear el esqueleto básico de la estructura del proceso de negocio.	Transición	Sequence Flow
		Flujo de mensaje	Message Flow
		Asociación	Association
Canales (Swimlane)	Los canales son mecanismos de organización de las actividades en categorías visuales separadas para ilustrar las diferentes áreas funcionales o responsables.	Área Funcional	Pools
		Fase	Lanes

Tabla 2 (Continuación)

ELEMENTO	DEFINICIÓN	VERSION ANTERIOR	NOMBRE BPMN
Artefactos (Artifacts)	Los artefactos son usados para proveer información adicional sobre el proceso. Otorgan flexibilidad a la notación para expresar diferentes contextos en forma apropiada.[15]	Objeto de Datos	Data Object
		Grupo	Group
		Anotación	Annotation

Fuente: BIZAGI BPMN (Bussiness Process Model and Notation)

Elementos de flujo

Eventos

Definición: un evento es algo que sucede durante el curso del proceso, afectan el flujo de proceso y normalmente tienen una causa (trigger) o resultado.

Representación: Los eventos son representados a través de círculos con centro vacío, lo cual permite incluir diferentes marcadores para diferenciarlos entre sí.
Tipos: los tipos de eventos se clasifican dependiendo de cuándo ellos afectan el flujo:

[15] BIZAGI BPMN (Bussiness Process Model and Notation) [En línea] <http://wiki.bizagi.com/es/index.php?title=BPMN>

Tabla 3. Tipos de eventos BPMN

TIPO DE EVENTO	NOMBRE BPMN	DEFINICIÓN	NOTACIÓN
Inicio	Start	Como su nombre lo indica, representa el punto de inicio de un proceso.	
Intermedio	Intermediate	Ocurren entre un evento de inicio y de fin. Afectará el proceso pero no lo iniciará o directamente finalizará.	
Fin	End	Indica cuando un proceso termina.[16]	

Fuente: BIZAGI BPMN (Bussiness Process Model and Notation)

Dentro de cada tipo de evento, estos a su vez se clasifican dependiendo del impacto en el flujo del proceso. Por ejemplo, algunos subtipos son: mensajes, timer, cancelación, error, etc. En Bizagi encontramos los siguientes:

[16] BIZAGI BPMN (Bussiness Process Model and Notation) [En línea] <http://wiki.bizagi.com/es/index.php?title=BPMN>

Tabla 4. Subtipos de eventos de inicio

NOMBRE BPMN	USO	NOTACIÓN
Message Start	Un proceso activo envía un mensaje a otro proceso específico para activar su inicio.	
Timer Start	Se puede fijar una hora-fecha específica (e.g. todos los lunes a las 9am) en la que se activará el inicio del proceso.	
Signal Start	Un proceso activo envía una señal y causa el inicio del proceso. Notar que la señal se envía a cualquier proceso que pueda recibir la señal, pero no es un mensaje (el cual tiene una fuente específica y un objetivo).[17]	

Fuente: BIZAGI BPMN (Bussiness Process Model and Notation)

Tabla 5. Subtipos de eventos de finalización

NOMBRE BPMN	USO	NOTACIÓN
Terminador	Es el fin del proceso. Solo existe uno por flujo. Si el proceso alcanza este evento, éste será cerrado.	

[17] BIZAGI BPMN (Bussiness Process Model and Notation) [En línea] <http://wiki.bizagi.com/es/index.php?title=BPMN>

Tabla 5 (Continuación)

NOMBRE BPMN	USO	NOTACIÓN
Cancelación	Este tipo de Fin es usado dentro de un subproceso de transacción. Éste indicará que la transacción debe ser cancelada y causará un Evento Intermedio de Cancelación adjunto a la frontera del subproceso.	
Error	Esta figura se usa para capturar errores, si están definidos o no. Todos los threads activos actualmente en un subproceso particular son en consecuencia terminados. El error será tomado por un Evento Intermedio de Error con el mismo Nombre, que está en la frontera de la actividad pariente más cercana.	
Señal	Este tipo de Fin indica que la señal será transmitida cuando el Fin haya sido alcanzado. Note que la señal es enviada a cualquier proceso que pueda recibir la señal y pueda ser enviada a través de los niveles del proceso, pero no es un mensaje (el cual tiene una fuente y un objetivo). [18]	

[18] BIZAGI BPMN (Bussiness Process Model and Notation) [En línea] <http://wiki.bizagi.com/es/index.php?title=BPMN>

Tabla 5 (Continuación)

NOMBRE BPMN	USO	NOTACIÓN
Mensaje	Este tipo de Fin indica que un mensaje se envía a un proceso o caso de actividad específica, al concluir el proceso.	

Fuente: BIZAGI BPMN (Bussiness Process Model and Notation)

Tabla 6. Subtipos de eventos intermedios

NOMBRE BPMN	USO	NOTACIÓN
Temporizador	Esta figura representa un mecanismo de retraso dentro del proceso. Este tiempo puede ser definido en una Expresión o como parte de la información del proceso (Fecha o duración en cualquier unidad de tiempo).	
Compensación	El Evento Intermedio indica que es necesaria una compensación. Entonces, se usa para "lanzar" el evento de compensación. Si una actividad es definida y ésta fue completada exitosamente, entonces la actividad será compensada.	
	Caminos de excepción del flujo ocurren fuera del flujo normal del proceso y se basa en un evento intermedio que ocurre durante el curso del proceso. En la figura me muestra el uso de línea de excepción con un subproceso y una actividad.	

Tabla 6 (Continuación)

NOMBRE BPMN	USO	NOTACIÓN
Mensaje	Un Evento Intermedio de Mensaje puede ser usado tanto para enviar como para recibir un mensaje. Cuando se usa para "lanzar" el mensaje, un marcador debe ser llenado. Cuando se usa para "atrapar" el mensaje el marcador debe estar sin llenar. Esto causa que el proceso continúe si éste estaba esperando por el mensaje o cambia el flujo para manejo de excepciones. Para atrapar y lanzar mensajes debe tener el mismo nombre.	
Enlace	Un Enlace es un mecanismo para conectar dos secciones de un Proceso. Los Eventos de Enlace pueden ser usados para crear situaciones de bucle o para evitar líneas de Secuencia de Flujo largas. Los usos de los Eventos de Enlace son limitados a un solo nivel de proceso.	
Señal	Las señales son usadas para enviar o recibir comunicaciones generales dentro y a través de los niveles de Proceso y entre Diagramas de Proceso de Negocio. Una señal BPMN es similar a una señal de bengala que se dispara al cielo para cualquiera que pudiera estar interesado y luego reaccionara. Entonces hay una fuente de la señal, pero ningún objetivo específico.	

Tabla 6 (Continuación)

NOMBRE BPMN	USO	NOTACIÓN
Error	Un Evento de Captura de Error Intermedio puede ser unido solamente a la frontera de una actividad. Notar que un Evento de Error siempre interrumpe la Actividad a la que está unido. [19]	

Fuente: BIZAGI BPMN (Bussiness Process Model and Notation)

Actividades

Definición: Las actividades representan trabajo o tareas realizadas por miembros involucrados dentro del proceso. Este elemento simboliza tareas manuales o automáticas llevadas a cabo por un usuario o un sistema externo. Las actividades pueden ser atómicas o no atómicas (compuestas).

Representación: Una actividad es representada por un rectángulo con bordes redondeados.

Tipos: Se clasifican en tareas y subprocesos. Los subprocesos se distinguen por un signo más en la parte inferior central de la figura. Los siguientes son los tipos de actividades:

[19] BIZAGI BPMN (Bussiness Process Model and Notation) [En línea] <http://wiki.bizagi.com/es/index.php?title=BPMN>

Tabla 7. Subtipos de actividades

NOMBRE BPMN	USO	NOTACIÓN
Tarea de Usuario	Es una tarea de “flujo de trabajo” donde un humano realiza una tarea que tiene que ser completada en cierta cantidad de tiempo. Se usa cuando el trabajo durante el proceso no puede ser descompuesto en un nivel más fino dentro del flujo. Tarea de usuario	
Tarea de Servicio	Una Tarea de Servicio es una tarea que usa algún tipo de servicio, que podría ser un servicio Web o una aplicación automática. Tarea de Servicio.	
Tarea de Recibir	Una Tarea de Recibir es una tarea simple para que llegue un mensaje. Una vez el mensaje haya sido recibido, la tarea es completada. Tarea de Recibir.	
Tarea de Enviar	Una tarea de Enviar es una tarea simple que es designada para enviar un mensaje a un proceso o caso específico. Una vez el mensaje haya sido enviado, la tarea es completada. Tarea de Enviar.	
Manual	Ésta es una Tarea que se espera que sea realizada sin la ayuda de algún motor de ejecución de proceso de negocio o alguna aplicación. Un ejemplo de esto puede ser una secretaria archivando documentos físicos. Tarea Manual.	

Tabla 7 (Continuación)

NOMBRE BPMN	USO	NOTACIÓN
Script	Una tarea de Script es una tarea automática en la que el servidor ejecuta un script. No tienen [20]interacción humana y no se conecta con ningún servicio externo. Tarea	
Subproceso	Un subproceso es una actividad compuesta incluida dentro de un proceso. Éste es compuesto dado el hecho que esta figura incluye un conjunto de actividades y una secuencia lógica (proceso), que indica que la actividad mencionada puede ser analizada a un nivel más fino. Se puede colapsar o expandir. Subproceso.	 
Subproceso Múltiple	Esta propiedad del subproceso permite la creación de instancias múltiples. Cada instancia representa una relación 1-N dentro del proceso. Subprocesos múltiples aplican sólo para procesos no embebidos. Subproceso Múltiple.	

[20] BIZAGI BPMN (Bussiness Process Model and Notation) [En línea] <http://wiki.bizagi.com/es/index.php?title=BPMN>

Tabla 7 (Continuación)

NOMBRE BPMN	USO	NOTACIÓN
Subproceso Transaccional	Un Subprocesos Transaccional facilita la implementación de escenarios de negocio con transacciones cuyas ejecuciones podrían durar muchos días o semanas hasta que el conjunto de actividades sea completado. Una transacción es realizada exitosamente cuando los cambios a ser implementados (actualización, adición o eliminación de registros) son grabados en la base de datos. Transaccional.	
Subproceso Embebido	Contiene un conjunto de actividades que no son independientes del proceso pariente, y por esto, comparten la misma información o datos.	

Fuente: BIZAGI BPMN (Bussiness Process Model and Notation)

Decisiones

Definición: Las Decisiones son usadas para controlar la divergencia y convergencia del flujo. Éstas determinan ramificaciones, bifurcaciones, combinaciones y fusiones en el proceso.

Representación: Son utilizadas por una figura de diamante. Marcadores internos mostrarán el tipo de control que se usa.

Tipos: Iconos en la figura de diamante indica el tipo de comportamiento del control de flujo. Tipos de control incluyen:

Tabla 8. Subtipos de elementos de decisión

TIPO DE DECISIÓN	DEFINICIÓN	NOTACIÓN
Decisión Exclusiva	Decisión basada en datos del sistema. El mismo elemento se usa para sincronizar esta figura. Decisión Exclusiva	
Decisión Basada en Evento	Puntos en el proceso en el que la decisión no está basada en los datos del proceso sino en eventos. Decisión Basada en Evento.	
Decisión Inclusiva	Inclusiva o multi-decisión. Uno o más caminos pueden ser activados. Uno o más caminos deben sincronizarse dependiendo de las actividades anteriores de la misma figura. Decisión Inclusiva	
Decisión Compleja	Elemento para controlar puntos de una decisión compleja. Por ejemplo, cuando 3 de 5 caminos deben esperar. Decisión Compleja.	
Decisión Paralela	Indica puntos en el proceso en el que varias ramas se desprenden o convergen en paralelo. El mismo elemento se usa para sincronizar esta figura. Decisión Paralela[21] .	

Fuente: BIZAGI BPMN (Bussiness Process Model and Notation)

[21]BIZAGI BPMN (Bussiness Process Model and Notation) [En línea] <http://wiki.bizagi.com/es/index.php?title=BPMN>

Conectores

Líneas de secuencia

Definición: Las líneas de secuencia son usadas para mostrar el orden en que las actividades serán llevadas a cabo en el proceso.

Representación: Son representadas por una flecha indicando “desde” y “hasta”.

Tipos: Los tipos de líneas de secuencia incluyen:

Tabla 9. Subtipos de líneas de secuencia

TIPO DE LINEA	NOMBRE ORIGINAL	DEFINICIÓN	NOTACIÓN
Línea normal	Normal Flow	La línea normal se refiere al flujo que se originan en el inicio, continúa a través de actividades hasta terminar en un evento de salida (por ejemplo el FIN).[22]	
Flujo Condicional	Conditional Flow	Este flujo tiene una condición asignada que define si el flujo es usado. Se puede asignar a cualquier figura en el proceso que requiera evaluar una condición para seguir cierto camino.	

Tabla 9 (Continuación)

[22] BIZAGI Conectores canales y artefactos [En línea] <http://wiki.bizagi.com/es/index.php?title=Artefactos_swimlanes_y_Objetos_Conectores#artefactos>

TIPO DE LINEA	NOMBRE ORIGINAL	DEFINICIÓN	NOTACIÓN
Línea por Default	Default Flow	Para decisiones basadas en datos o decisiones inclusivas, un tipo de camino del flujo es el de condiciones por “default”. Este tipo de transiciones se presenta únicamente si todas las otras condiciones son no verdaderas en un mismo instante. Una vez asignada la condición “Else” a la transición, se verá la flecha como aparece en el dibujo a la derecha.	

Fuente: BIZAGI Conectores canales y artefactos

Canales (Swimlanes)

En determinadas ocasiones ocurre que un diagrama de actividad se expanda a lo largo de más de un entidad o actor, cuando esto ocurre el diagrama de actividad es particionada en canales (swimlines), donde cada canal representa la entidad o actor que está llevando a cabo la actividad.[23]

Los canales se utilizan como mecanismo de organización de las actividades en categorías visuales separadas para ilustrar los diferentes responsables.

Tipos: En BPM se utilizan dos tipos: Área Funcional y Fase.

[23] BIZAGI Conectores canales y artefactos [En línea] <http://wiki.bizagi.com/es/index.php?title=Artefactos_swimlanes_y_Objetos_Conectores#artefactos>

Funcional

Definición: Representa un participante en un proceso. Se le conoce también como área funcional.

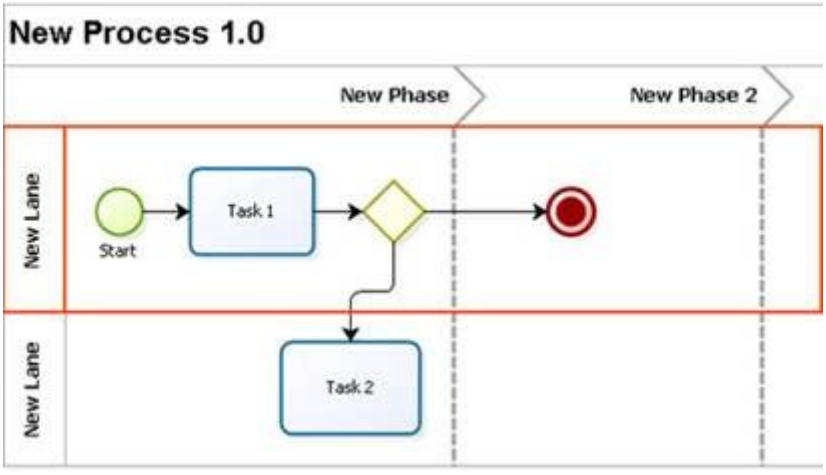
Representación: Partición que se extiende a lo largo del proceso en forma horizontal.

Fase

Definición: Es una subpartición dentro de un pool y se extenderá sobre el pool en forma horizontal o vertical. En Bizagi existen los lanes verticales y se conocen también como fases. Los lanes son usados para organizar y categorizar actividades.

Representación: Línea vertical que separa los diferentes estados dentro del proceso como se puede ver en la figura 3.[24]

Figura 3. Ejemplo de utilización de una fase



Fuente: BIZAGI Conectores canales y artefactos

[24] BIZAGI Conectores canales y artefactos [En línea] <http://wiki.bizagi.com/es/index.php?title=Artefactos_swimlanes_y_Objetos_Conectores#artefactos>

Artefactos

Los Artefactos son objetos gráficos que proveen información de soporte sobre el Proceso o elementos dentro del proceso. Sin embargo, estos no afectan directamente el flujo del proceso.

Un Artefacto no debe ser un objetivo para el Flujo de Secuencia.

Grupos

Definición: Se utiliza para agrupar un conjunto de actividades, ya sea para efectos de documentación o análisis, sin embargo, no afecta la secuencia del flujo.

Representación: Rectángulo redondeado dibujado con línea segmentada.

Anotaciones

Definición: Son mecanismos para que un modelador pueda proveer información adicional en un diagrama de BPMN.

Representación: Cuadro para incluir información.

Objeto de datos

Definición: Provee información sobre cómo los documentos, datos y otros objetos son usados y actualizados durante el proceso. Se puede usar para representar objetos electrónicos y físicos.

Representación: Icono de documento.[25]

[25] BIZAGI Conectores canales y artefactos [En línea] <http://wiki.bizagi.com/es/index.php?title=Artefactos_swimlanes_y_Objetos_Conectores#artefactos>

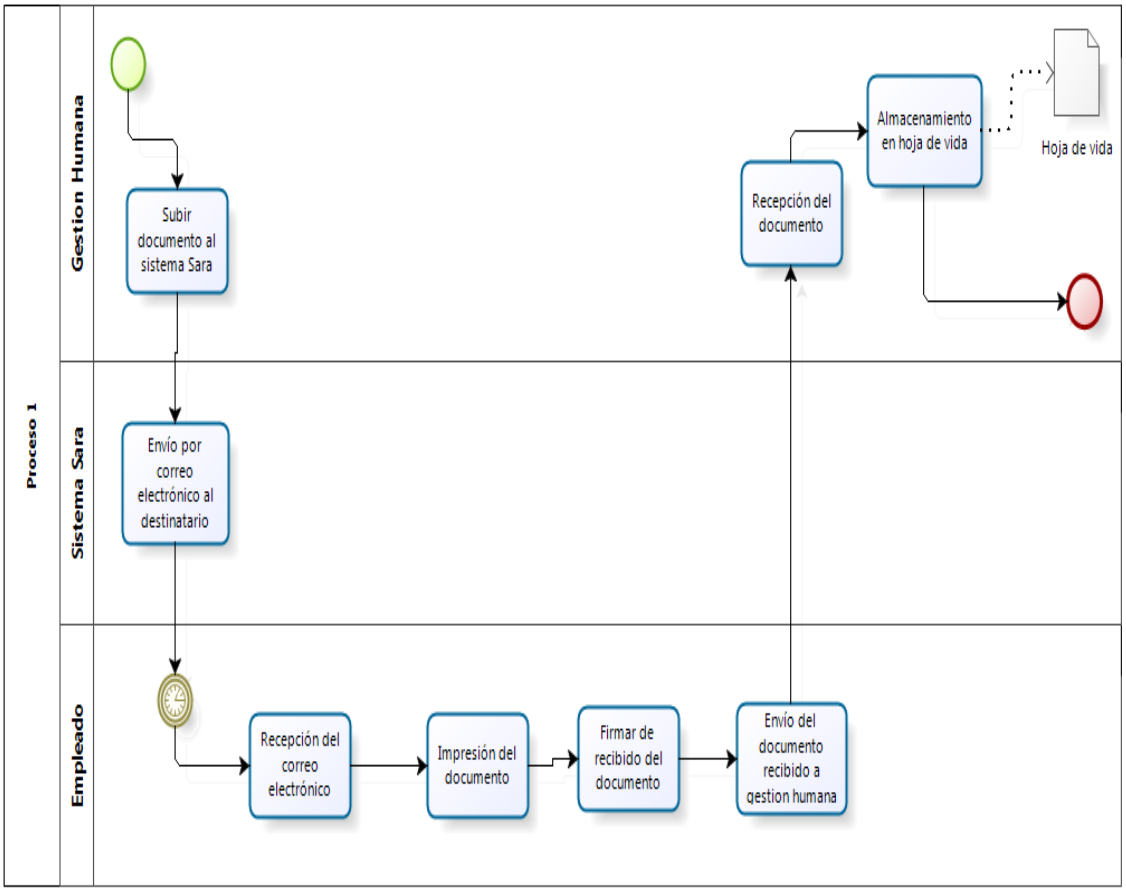
2.1.2 Modelado de la solución propuesta con BPMN. Se realizó una búsqueda para profundizar y aplicar el concepto de flujo de trabajo o Workflow con fines de realización de dos modelos: el primero con el motivo de analizar la forma en la cual se realiza el proceso de envío de memorando por parte de gestión humana actualmente sirviendo este modelo como base para elaborar un segundo modelo, el cual este serviría como una propuesta a una solución alternativa para el proceso de envío de memorandos para que este pueda hacerse de una forma virtual pero que esta sea segura.

Se tuvo una charla con la directora del departamento gestión humana de la Universidad Autónoma de Bucaramanga Nimia Arias Osorio con el fin de obtener una mejor comprensión del funcionamiento de los procesos que se realizan dentro de este departamento, en donde se encontró la aplicabilidad de la criptografía asimétrica dentro del campo del envío de memorandos de vacaciones a sus empleados en donde el proceso actual que se realiza es el siguiente: Una vez el documento esté preparado, es subido dentro de una plataforma que se maneja dentro del departamento conocida como Sara, dentro de esta, como una parte de sus funciones, envía el documento por medio de correo electrónico, hacia la persona destinataria, en donde esta persona recibe el documento y lo imprime, después el documento es firmado y enviado de vuelta al departamento de gestión humana, proceso que si se analiza, posee un alto consumo de papel, debido a envía un memorando por cada empleado, en donde al cabo de una año la cantidad de papel consumida se hará notable

Para la realización de estos Workflow se harán a través de la notación BPMN, la cual es fácil de comprender su lógica que realizan los procesos, y en donde se utiliza para dar explicación de cómo funciona la solución propuesta.

Utilizando el software Bizagi Process Modeler para la realización de workflows con notación BPMN, se realizó un modelo que representa el procedimiento del envío de memorandos de vacaciones por parte de gestión humana.

Figura 4. Diagrama básico en BPMN del proceso de envío de memorandos de vacaciones en gestión humana



Fuente: Autor del proyecto

A través de la información obtenida dentro de los capítulos anteriores se ha elaborado un modelo en BPMN el cual representa el funcionamiento del modelo propuesto.

En primer lugar el usuario accede al sistema, en donde si el usuario no posee una cuenta ya registrada, el usuario podrá ingresar sus datos para registrar un nuevo usuario y además crear el conjunto de llaves para realizar el cifrado y descifrado de documentos, cuando el usuario accede le sistema el usuario que desee enviar un documento a otro usuario debe elegir la opción de enviar un documento, en donde elegirá el usuario destino y acto seguido, subirá el documento que se desee enviar y confirmar para poder enviar el documento al usuario destino.

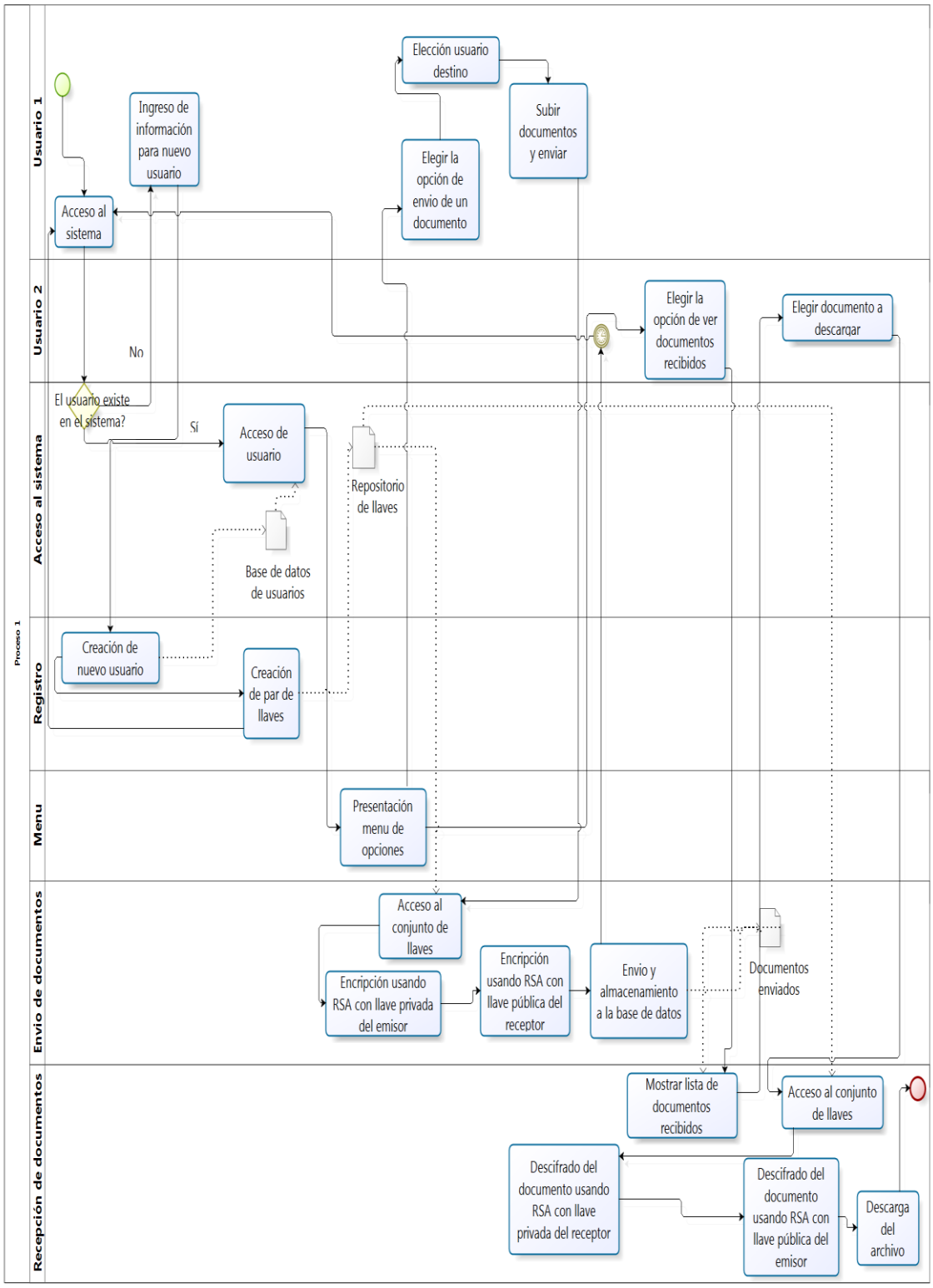
En este momento el sistema se encargará de procesar la información suministrada por el usuario para realizar la encripción necesaria y el envío al usuario correspondiente.

El sistema accederá al conjunto de llaves correspondiente del usuario emisor, estas se encuentran dentro de un repositorio de llaves almacenado dentro de una base de datos y comenzará a realizar el proceso de encripción del documento, el sistema realiza un proceso de encripción doble para poder completar este proceso, en primer lugar se realizar una encripción utilizando el algoritmo RSA utilizando la llave privada del emisor, una vez realizada dicha encripción el sistema buscará las llaves del receptor en el repositorio de llaves y acto seguido realizará el proceso de encripción utilizando el algoritmo RSA utilizando la llave pública del receptor, una vez el sistema ha terminado de realizar los dos procesos de encripción previamente mencionados, se guardará el documento encriptado en la base de datos con los datos del usuario destino para que sea este el que pueda recibirlo.

Para que el usuario destino puede recibir el documento enviado, este debe acceder al sistema ingresando su usuario y contraseña, una vez dentro del sistema, deberá elegir la opción de ver los mensajes recibidos, una vez elegida la opción, el usuario destino podrá ver los mensajes que ha recibido y quien ha sido el emisor del mensaje además de un link para realizar el proceso de descarga, una vez elegido el documento a descargar, el sistema realizará el proceso del descifrado del documento.

Para realizar este proceso el sistema accederá al conjunto de llaves del receptor en donde se iniciará el proceso de descifrado utilizando el algoritmo RSA utilizando la llave privada del receptor del mensaje, acto seguido el sistema accederá al conjunto de llaves del emisor y realizará el proceso de descifrado utilizando el algoritmo RSA y utilizando su llave pública para realizar el proceso de descifrado, una vez realizado el doble proceso de descifrado, el documento estará listo para la descarga, apareciendo la opción al usuario receptor de guardar el documento en donde desee.

Figura 5. Modelo en BPMN que explica la solución alternativa para el envío de notificación de vacaciones



Fuente: Autor del proyecto

3. DESARROLLO Y PRUEBAS DEL MODELO TECNOLÓGICO PARA EL INTERCAMBIO SEGURO DE DOCUMENTOS

A partir de la información recolectada en el capítulo 1 y la definición de la técnica basada en criptografía a utilizar definida en el en el subcapítulo 1.4, se han realizado diferentes pruebas para realizar el proceso de cifrado y descifrado de documentos usando el lenguaje de programación Java, en donde siguiendo los conceptos de criptografía asimétrica se puede lograr autentificación del usuario a través del cifrado utilizando la llave privada del emisor y donde el receptor descifra el mensaje utilizando la llave pública del emisor.

Por otro lado se puede lograr que el mensaje enviado solo pueda recibido a un solo individuo, para el caso en que se requiera lograr seguridad en el mensaje evitando que este pueda ser interceptado por un tercero, esto es logrado a través del cifrado con la llave pública del receptor en donde el documento solo puede ser descifrado utilizando la llave privada del mismo.

Finalmente se pudo lograr un proceso combinado de los dos métodos anteriores, en el cual, a través de un cifrado doble utilizando la llave privada del emisor y la pública de receptor y descifrándolo haciendo uso de la llave pública del emisor y la privada del receptor permite que el documento a enviar sea resistente a intercepciones por parte de terceros y además de que el receptor puede identificar al emisor utilizando la llave que le corresponde a este.

Este proceso fue logrado a través de la utilización de un conjunto de llaves que poseen el algoritmo de cifrado RSA de 2048 bits para el cifrado y utilizado en conjunto con el algoritmo de cifrado AES para permitir un cifrado rápido y que permita realizar su cifrado en documentos de tamaño considerable, En donde para que las llaves puedan ser reconocidas y utilizadas por java deben estar en el formato PKCS8# y DER[26].

[26] LONES, Michael. Encrypting files with public key encryption in Java [En línea] <http://www.macs.hw.ac.uk/~ml355/lore/pkencryption.htm>

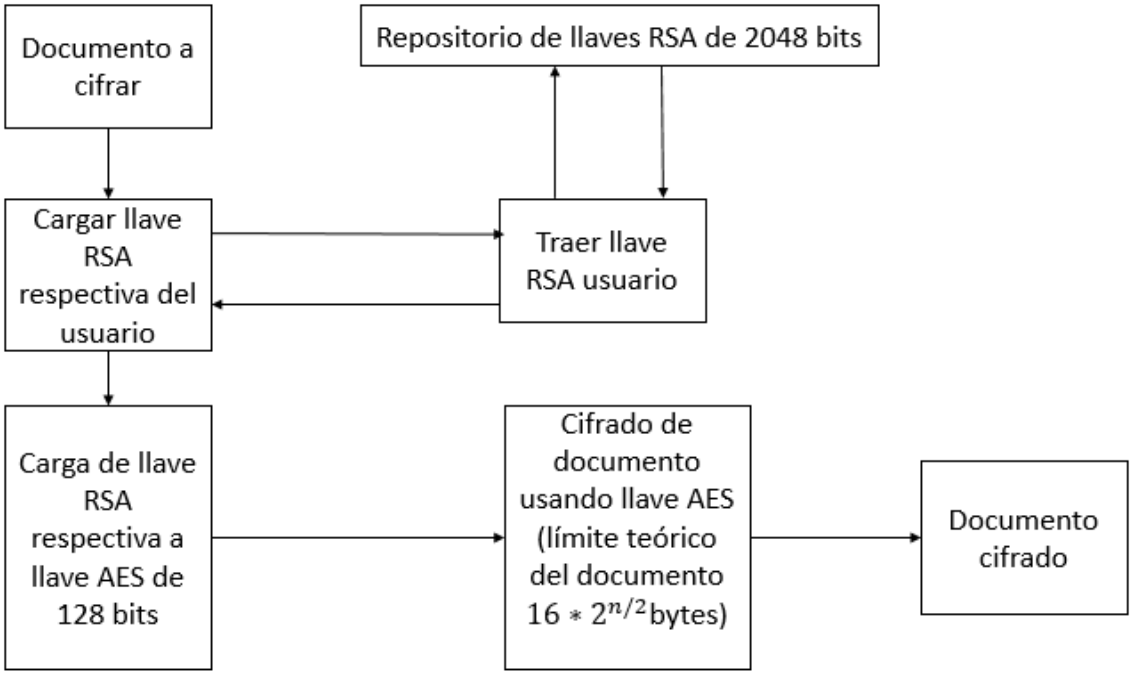
3.1 USO COMBINADO DE ALGORITMOS RSA Y AES

La utilización de criptografía simétrica y asimétrica es frecuentemente utilizada para la elaboración de sistemas basados en criptografía, por otro lado, resuelve un inconveniente de la solo utilización de un algoritmo de criptografía asimétrica como RSA que es la encripción de archivos de pequeño tamaño, inconveniente que no es poseído por un algoritmo de criptografía simétrica, en la siguiente figura se puede observar de forma sencilla la interacción que tienen estos dos algoritmos para el cifrado de un documento:

La interacción entre estos dos algoritmos para el cifrado de un documento consiste en primer lugar en la carga de una llave RSA respectiva de un usuario la cual utiliza 2048 bits y posee un límite teórico de 4096 bits, esta llave puede ser la llave pública o privada dependiendo de cómo se desee utilizar RSA, acto seguido, se realiza la creación de la llave AES de 128 bits, en donde estará contenida la llave RSA utilizada, esta llave creada será utilizada para realizar el proceso de cifrado del documento, el tamaño del documento a cifrar es bastante grande, el límite teórico definido para la encripción de un archivo a través del algoritmo AES para lograr la generación de llaves únicas es de $2^{n/2}$ [27]bloques de cifrado, en donde cada bloque es de 16 bytes y en donde n representa la cantidad de bits utilizados para el algoritmo AES, en donde para este caso en que se aplica, los documentos tendrán un límite teórico de $16 * 2^{64}$ bytes, lo cual representa una cantidad bastante grande de información permitida para ser cifrada, al final del proceso se obtiene como resultado el documento cifrado utilizando una llave AES cuyo contenido está conformado por el contenido de la llave RSA.

[27] INFORMATION SECURITY After how much data encryption (AES-256) we should change key? [En línea] <http://security.stackexchange.com/questions/30170/after-how-much-data-encryption-aes-256-we-should-change-key>

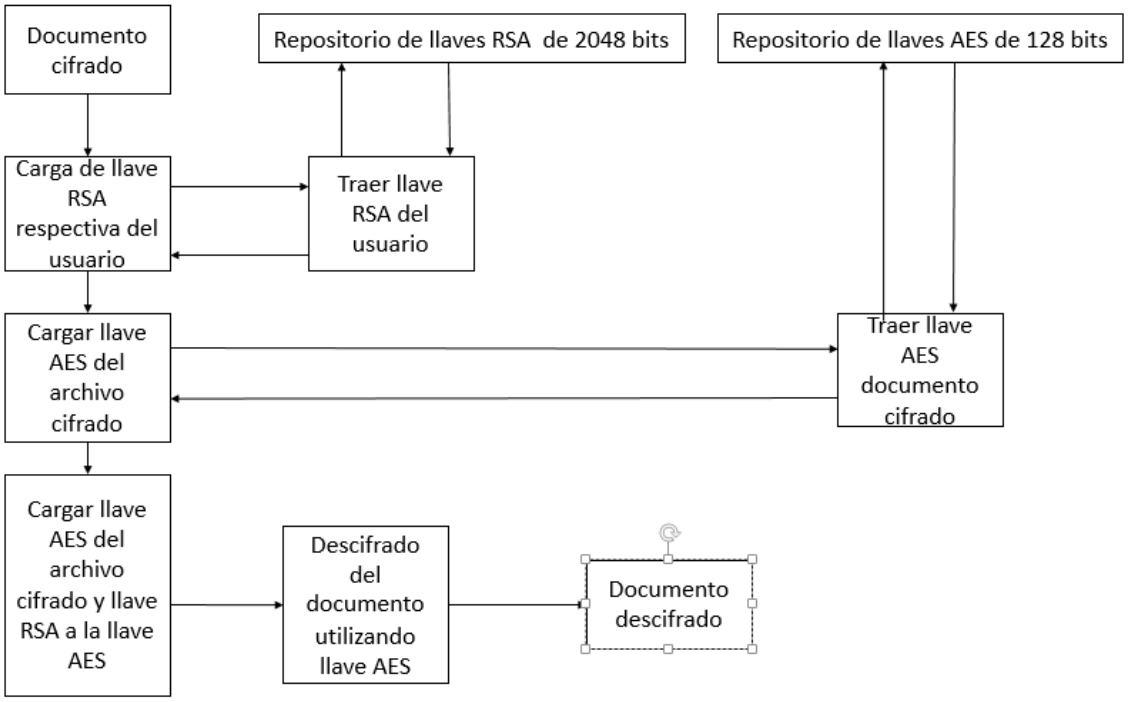
Figura 6. Proceso simplificado de interacción entre RSA y AES para cifrado de documentos



Fuente: Autor del proyecto

Para el proceso de descifrado es necesario la carga de la llave RSA de 2048 bits respectiva del usuario, es decir, si el documento se ha encriptado un documento con la llave pública se necesitará la privada y viceversa; Además se necesita cargar la llave AES de 128 bits generada durante el cifrado del documento, acto seguido se carga la llave AES del archivo cifrado y la llave respectiva RSA a la nueva llave AES creada a partir de estas dos, en donde como procedimiento final se utiliza esta llave creada a partir del proceso anterior para realizar el proceso de descifrado utilizando el algoritmo AES para el descifrado, obteniendo como resultado el documento original listo para ser visualizado.

Figura 7. Proceso simplificado de interacción entre RSA y AES para descifrado de documentos



Fuente: Autor del proyecto

Para mayor información acerca de la utilización conjunta de estos dos algoritmos puede ver el artículo de investigación de Palanisamy y Jeneba[28]

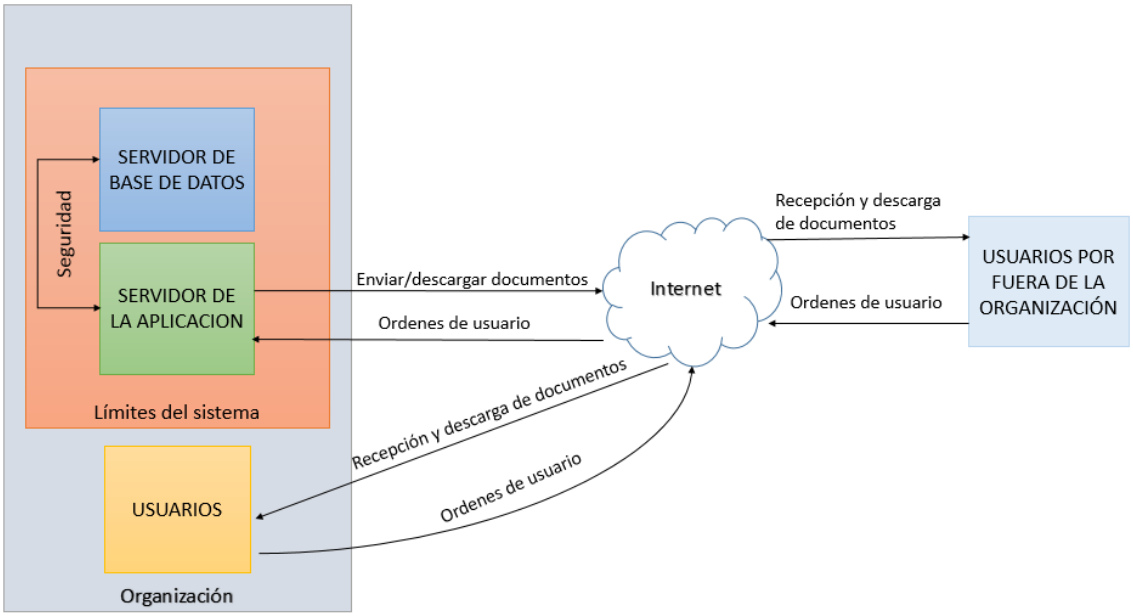
3.2 DEFINICIÓN DEL MODELO TECNOLÓGICO PARA EL INTERCAMBIO SEGURO DE DOCUMENTOS

Con la información recogida en los capítulos anteriores, se define el modelo tecnológico que sirve como alternativa para el proceso de envío seguro de documentos, cuyo proceso de interacción entre los usuarios ha sido anteriormente explicado en el capítulo 5.1.2 (Ver figura 5).

[28] PALANISISAMY V, JENEBA MARY. Hybrid cryptography by the implementation of RSA and AES En: International journal of current research [En línea] (Abril del 2011) < http://www.journalcra.com/sites/default/files/Download%20546.pdf >

El modelo tecnológico consiste en la utilización de dos servidores, un servidor de la aplicación, en donde se encontrará todo el software necesario que se necesita para que la aplicación funciona correctamente, en donde esta va a poder enviar y cifrar documentos además de poder descifrar y descargar los documentos deseados; Por otro lado se encuentra el servidor de base de datos, en este servidor se almacenará toda la información respectiva que utilice el sistema, es decir, las diferentes cuentas de usuario, las llaves respectivas de cada uno de ellos y los documentos que han sido enviados a cada uno de los mismos; Los servidores de aplicación y de base de datos se comunican entre ellos para el proceso de cifrado y descifrado de información que es donde se manejará la parte de seguridad de información del sistema.

Figura 8. Modelo tecnológico para el envío seguro de documentos



Fuente: Autor del proyecto

El usuario realizará las órdenes que desea hacer dentro del sistema, entre estas órdenes se encuentran: Enviar documentos, ver documentos recibidos y descargar documentos, en donde el sistema retornará la respuesta elegida por el usuario, además, como se puede ver en la figura 8, el usuario puede acceder al sistema dentro y fuera de la organización a través de internet.

A continuación se explicará la definición del modelo a partir de su arquitectura a nivel de aplicaciones y el hardware necesario a disponer para la implementación de este modelo.

3.2.1 Arquitectura de la aplicación requerida para el modelo. Para el procedimiento del cifrado y descifrado de documentos, se utilizan las librerías java crypto y java security como base para la creación del código de cifrado y descifrado esta librería está contenida dentro de la librería principal de Java JDK que para el desarrollo del prototipo de la aplicación se utilizó la versión 1.6, este funcionamiento será explicado a través de diagramas de secuencia.

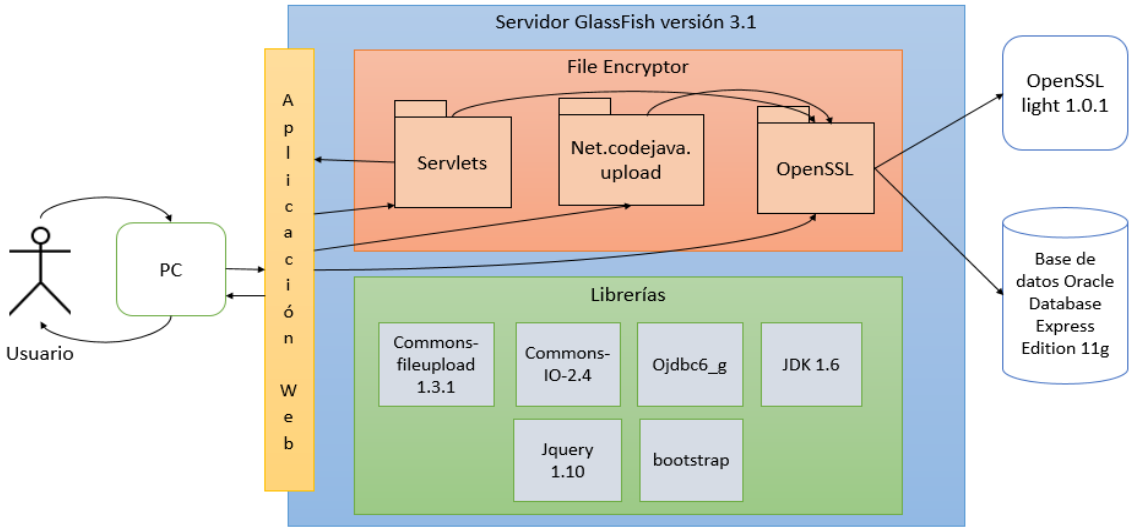
Las llaves pertenecientes a cada usuario son creadas a través de la herramienta de software libre OpenSSL, los conjuntos de llaves creados están guardados digitalmente dentro de una base datos, en donde se ha utilizado el motor de base de datos de Oracle para gestionar las llaves además de los documentos encriptados por estas llaves.

Estas llaves son utilizadas por la aplicación principal, la cual se encarga de realizar los procesos de cifrado y descifrado de documentos, utilizando las llaves requeridas para el proceso de forma adecuada, de esta manera los usuarios no necesitan ningún tipo de interacción compleja para realizar la encripción y desencripción del archivo, la aplicación se encargará de realizar estos procesos

Por otro lado para el procedimiento de subida de archivos utiliza la librería Apache FileUpload versión 1.3.1 para este proceso, la cual permite ser adaptada de forma de que los archivos subidos por el usuario puedan ser encriptados y luego subidos a la base de datos.

El usuario podrá acceder al servicio brindado por la aplicación a través de una aplicación web que utiliza a GlassFish versión 3.1 como servidor y el cual permitirá ofrecer el servicio a la aplicación de encripción de documentos que tendrá el nombre de File Encryptor.

Figura 9. Diagrama de la arquitectura de la aplicación



Fuente: Autor del proyecto

3.2.2 Hardware requerido para la aplicación del modelo tecnológico. Para el cálculo de requisitos de hardware para la aplicación del modelo tecnológico se tuvo en cuenta una cantidad promedio de 800 empleados trabajando dentro de la universidad autónoma de Bucaramanga con un tiempo permanencia promedio de 10 años, además se tuvo en cuenta una tamaño promedio de memorando, el cual se estima que posee un tamaño máximo aproximado 300 Kb en donde para el proceso de envío de memorando de vacaciones es realizado una vez por año y se utiliza para envío y respuesta del memorando ocupando una cantidad promedio de 600 Kb por empleado.

Siguiendo estos cálculos se estimó un consumo promedio anual de 468 Mb anuales en espacio ocupado en base de datos.

Si se piensa sobre una utilización del modelo para el envío de memorandos para otros tipos de memorandos el costo de disco duro será más alto y por lo tanto un aspecto a tener en cuenta en la implementación del modelo.

El hardware necesario para la utilización continua y extendida de la aplicación consistirá de un servidor dedicado de base datos , el cual deberá tener como requisitos mínimos un disco duro de 100 Gb y una memoria RAM de 4 Gb, esto se encuentra sustentado debido a una utilización continua de envío de memorandos de envío y respuesta, el cual permite un almacenamiento extenso de documentos pensado para un uso ampliado del modelo en donde no solo se aplique al proceso del envío de memorando de vacaciones sino también a otros memorandos por parte de gestión humana y cuyo costo de almacenamiento en disco será mayor.

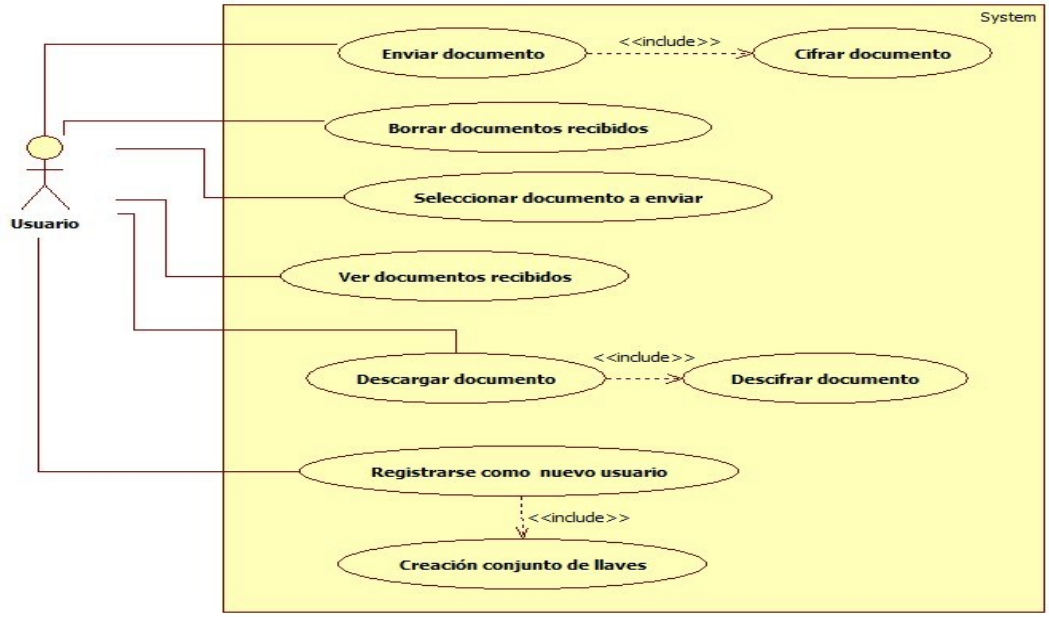
Por otro lado el hardware requerido para el servidor de aplicación requerirá un ancho de banda mínimo de 100 Mbps, esto es debido al posible elevado número de gente que pueda estar utilizando la aplicación en determinado momento, en donde junto al servidor de base de datos su uso pueda ser extendido para el intercambio de otros memorandos por parte de gestión humana además de una memoria RAM de 4 Gb en requerimientos de disco no es necesario ningún disco duro en particular debido a que el almacenamiento de información será realizado por el servidor de base de datos.

3.3 FUNCIONALIDADES DE LA APLICACIÓN FILE ENCRYPTOR

La aplicación File Encryptor cumplirá las siguientes funcionalidades que se pueden ver dentro del siguiente diagrama de casos de uso, en donde como se puede ver en la figura 7, los procesos que poseen una línea punteada cuya punta está conectada a otro proceso con la palabra “include” sobre la línea punteada representan a un procesos que debe realizarse para el cumplimiento de la funcionalidad a la cual se encuentra conectada en el otro extremo, en donde el sistema se hará cargo de la realización de estos procesos sin necesidad de intervención humana dentro del proceso, de forma que le brindará facilidad de uso a los usuarios, las funcionalidades que el usuario podrá realizar en File Encryptor son las siguientes: Envío de documentos, borrado de documentos

recibidos por parte del usuario, listar los documentos que un usuario ha recibido, descargar el documento que el usuario desee y registrarse como un nuevo usuario en File Encryptor

Figura 10. Diagrama de casos de uso del prototipo del sistema



Fuente: Autor del proyecto

File Encryptor tendrá en cuenta el proceso para la nueva creación de usuarios en donde también se creará el conjunto de llaves respectivo para cifrar y descifrar mensajes

File Encryptor posee un proceso para registrar nuevos usuarios al sistema creando a su vez las llaves necesarias para el proceso de cifrado y descifrado de documentos, en primer lugar el usuario registra sus datos dentro de la zona de registro de usuario y envía la información, después de esto la información enviada para validar que la información suministrada este completa y sea válida, el sistema no creará dos usuarios del mismo nombre ni creará usuarios con información incompleta, una vez validada la información el sistema llamará una función la cual utilizará esta información suministrada y utilizará la librería

OpenSSL para crear las llaves respectivas del usuario y almacenar dichas llaves junto al nuevo usuario creado, y de esta manera, asociar a cada usuario con su respectivo conjunto de llaves, para más información ver Anexo A. Diagrama de secuencia para el registro de usuario y creación de llaves respectivas

File Encryptor además posee el proceso de envío de documentos a un usuario destino, dentro de este proceso el usuario escribirá el nombre de usuario a enviar el documento respectivo, al tenerlo escrito el sistema realizará una búsqueda en la base de datos para encontrar usuarios que coincidan con la búsqueda del usuario en donde el usuario seleccionará el usuario de la lista de usuarios encontrados al que desee enviar el documento, una vez seleccionado el usuario podrá elegir el documento que desea enviar y enseguida presionar el botón de enviar documento para realizar la preparación y envío del documento, para más información ver Anexo B. Diagrama de secuencia que explica el proceso de envío de documentos

Para el proceso de cifrado de un documento se hace llamado a la clase FileEncryption la cual permite prepara una llave AES de 128 bits definida dentro de esta clase, la clase FileEncryption hará un llamado a la función saveKeyDB para realizar la carga de la llave AES proceso previamente explicado en el capítulo 3.1 y el cual permite una encripción de documentos de tamaño grande una vez la llave está cargada el cifrador realiza el proceso de encripción transmitiendo la información de entrada, en este caso, el documento a encriptar y la convierte a una salida cifrada, dicha información cifrada es almacenada por File Encryptor dentro de la base de datos, para mayor comprensión del proceso de encripción ver para la explicación del proceso a través de un diagrama de secuencia.

El usuario puede ver los mensajes que ha recibido, en este proceso el usuario que acceda a la sección de mensajes recibidos, el sistema realizará una consulta en la base de datos para traer los documentos enviados al usuario mostrándolo en una tabla junto al nombre del usuario emisor y un link para descargar el video. Para más información del proceso de mostrar los documentos ver Anexo D.

Diagrama de secuencia que explica el proceso de mostrar los documentos recibidos por un usuario

Un usuario podrá eliminar los documentos recibidos que el usuario desee para realizar este proceso, el usuario selecciona los mensajes que desee borrar y elige la opción de borrar, el sistema utilizará los id que poseen cada uno de los mensajes a través de una consulta de borrado en la base de datos en donde se borrarán cada uno de los mensajes cuyos id hayan sido seleccionados por el usuario, en donde al final del proceso los mensajes enviados a eliminar ya no aparecerán en la lista de mensajes recibidos, para mayor información ver Anexo E. Diagrama de secuencia que explica el proceso de borrado de documentos recibidos por un usuario.

El proceso de descarga de documentos comienza con el descifrado del documento que se desee descargar el cual se envían los usuario emisor y destino para realizar el proceso, una vez se termina el proceso de descifrado el sistema genera el contenido descifrado prepara el contenido para la descarga según el formato original en que se encontraba el documento para generar la descarga de manera adecuada, esto generará una ventana de descarga para que el usuario guarde el documento en donde este desee, para más información sobre el proceso ver Anexo F. Diagrama de secuencia que explica el proceso de descarga de documentos

Para una explicación más detallada del proceso a través de diagramas de secuencia

El proceso utilizado para el descifrado del documento utilizado en File Encryptor se toma como requisito de entrada el documento que se desea descargar, estos documentos están asociados por un id el cual los identifica, además es necesario saber los usuario emisor y destino información que puede ser traída de la base de datos fácilmente cuando se conoce el id del envío respectivo, una vez se tienen estos requisitos el sistema traerá las llaves de los usuarios emisor y

destino en donde realizará en primer lugar el proceso de desencripción RSA utilizando la llave privada del receptor, en este proceso, el cual comparte una alta similitud junto con el proceso de encripción, se prepara una llave AES en la cual se inscribe en ella la llave privada RSA del emisor, acto seguido se utiliza un descifrador, el cual utilizando la llave AES conteniendo la llave RSA realiza un proceso de transferencia de contenido desde el archivo almacenado en base de datos previamente cifrado a un archivo.

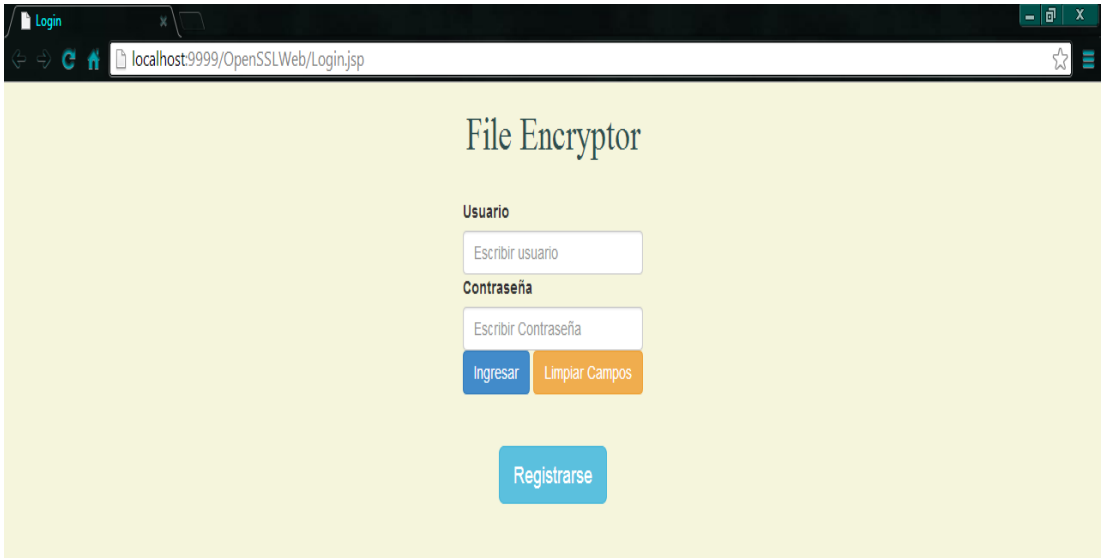
Ya descifrado de la encripción por el conjunto de llaves del emisor, para poder completar el proceso, este mismo proceso se repite para el conjunto de llaves del emisor, con la diferencia en donde este utiliza la llave pública del emisor para realizar el descifrado y cuyas funciones son diferentes pero en esencia cumplen la misma función, una vez terminado el doble descifrado utilizando las llaves RSA del emisor y el receptor el documento ya está listo para ser descargado.

Para mayor información respecto al proceso de descifrado de documentos ver Anexo G Diagrama de secuencia que explica el proceso de desencripción de un documento
que permite explicar el proceso de forma más explícita a través de diagramas de secuencia

3.4 FUNCIONAMIENTO DE LA APLICACIÓN FILE ENCRYPTOR

File Encryptor comenzará con una ventana de acceso al sistema en donde el usuario digitará su usuario y contraseña para acceder al sistema, en caso de que el usuario no posea una cuenta

Figura 11. Ventana de acceso al sistema



Fuente: Autor del proyecto

Para los usuarios que no posea una cuenta deberán hacer clic sobre el botón “Registrarse”, a continuación aparecerá una ventana para registrar la información del usuario seguido del botón “Enviar” para enviar la información de usuario agregada y en donde el sistema agrega el usuario a la base de datos y también creará el conjunto de llaves correspondiente al usuario.

Figura 12 Ventana de registro de usuario

Fuente: Autor del proyecto

Una vez el usuario este registrado, el usuario puede acceder al sistema en donde aparecerán dos opciones principales: “Enviar un documento” y ver “documentos recibidos”

Si el usuario desea enviar un documento cifrado a otro usuario, el usuario tendrá que hacer clic sobre la opción “Enviar un documento” haciendo aparecer una barra de búsqueda en donde el usuario escribirá el nombre del usuario a enviar, el sistema posee una función de autocompletar información para facilitar la búsqueda de usuarios.

Figura 13. Ventana de selección de usuario

Fuente: Autor del proyecto

Una vez escrito el nombre el usuario deberá dar clic en el botón enviar y confirma que el usuario buscado es el correcto al hacer clic sobre el botón que aparecerá al lado de su nombre.

Figura 14. Confirmación del usuario buscado

Fuente: Autor del proyecto

Una vez seleccionado el usuario destino, el emisor deberá seleccionar el mensaje a enviar, una vez seleccionado, el usuario deberá hacer clic en el botón enviar, el sistema cifrará el documento para proteger su contenido.

Figura 15. Selección del documento a enviar

Fuente: Autor del proyecto

Si el usuario necesita ver que documentos ha recibido, deberá hacer clic sobre el botón “Ver documentos recibidos” que está ubicado en el menú principal, a continuación aparecerá una tabla mostrando los mensaje que dicho usuario ha

recibido, además mostrará el usuario que envió el documento respectivo seguido de un link de descarga, el sistema utilizará las llaves del usuario emisor y destino para realizar el descifrado correspondiente antes de realizar la descarga del documento.

Figura 16. Ventana de mensajes recibidos del usuario

Fuente: Autor del proyecto

3.5 REALIZACIÓN DE PRUEBAS SOBRE FILE ENCRYPOR

Para probar el funcionamiento correcto de la aplicación File Encryptor se realizaron 3 pruebas para determinar el correcto funcionamiento del usuario y la creación de llaves, cifrado y descifrado de documentos y la garantía de que solo el usuario destino tenga acceso al documento enviado.

Para la primera prueba se decidió crear un nuevo usuario, de nombre Andrés Castro para poder ingresarlo al sistema.

Figura 17. Creación de usuario de prueba

Fuente: Autor del proyecto

Figura 18. Menú principal usuario de prueba

Fuente: Autor del proyecto

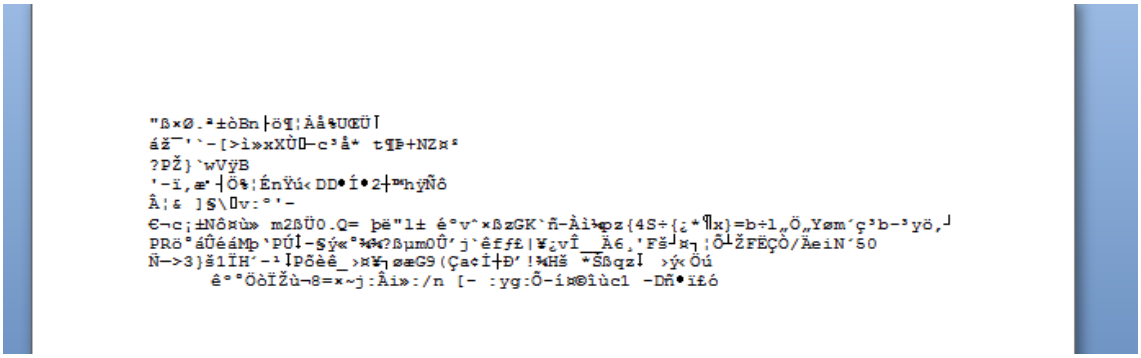
En donde se le envió un documento a otro usuario destino de forma que al momento en que el usuario destino revise los documentos que este ha recibido identificando como usuario emisor del mensaje a Andrés Castro.

Figura 19. Recepción del documento del usuario de prueba

Fuente: Autor del proyecto

Para asegurar que solamente el usuario destino tenga acceso al documento enviado por el usuario Andrés Castro se ha realizado una tercera prueba, en donde se alterado la base de datos para hacer que el documento llegue a un usuario erróneo, al momento de que el usuario no autorizado descargue el documento, el documento no estará descifrado, esto es debido a que File Encryptor utilizará el conjunto de llaves del usuario destino erróneo y por lo tanto el contenido del documento estará irreconocible para el usuario que ha descargado el documento, este mismo proceso también se realizó para el caso contrario en donde, se ha alterado la base de datos para informar que el usuario emisor del documento es otro distinto a Andrés Castro, para ambos casos anteriormente explicados el documento descargado seguirá cifrado y por lo tanto se ha asegurado que el envío se ha alterado.

Figura 20: Contenido cifrado descargado por un usuario no autorizado



Fuente: Autor del proyecto

4. CONCLUSIONES

El uso de llaves que se apoyan en el concepto de criptografía asimétrica permite que un mensaje o documento posea un mayor nivel de seguridad, de manera de que el documento sea más resistente a intercepciones por parte de terceros, debido a que se debe tener conocimiento del contenido de dos llaves distintas que se complementan para poder hacer el respectivo descifrado del documento, además, un uso apropiado de las llaves permiten asegurar que el documento pueda ser accedido solamente por el usuario destino y ofrecer seguridad a este garantizando que el documento fue enviado por el usuario quien dice ser, y por lo tanto permite lograr un intercambio seguro de documentos.

Java posee librerías disponibles para manejar criptografía, para poder utilizarla es necesario que las llaves a utilizar se encuentren en el formato PKCS8#, la utilización de la herramienta de software libre OpenSSL permite crear llaves y pasarlas a este formato, OpenSSL también permite definir el algoritmo de cifrado y la cantidad de bits de cifrada deseada para las llaves, siempre y cuando se encuentre dentro de la cantidad aceptada por el algoritmo de cifrado, por ejemplo, el algoritmo DES tiene un tamaño máximo de 64 bits mientras que el algoritmo RSA posee un tamaño máximo aceptado de 4096 bits.

Se encontraron inconvenientes al momento de cifrar documentos utilizando el algoritmo RSA, puesto a que el uso de este no permite archivos de gran tamaño, como solución a este problema, se puede utilizar un uso combinado de los algoritmos RSA y AES, el cual al combinar estos dos algoritmos permite utilizar el algoritmo RSA para cifrar documentos grandes.

5. TRABAJOS FUTUROS

Existe la posibilidad de trabajar sobre el prototipo para agregar una mejora en el sistema de envío de mensajes en donde se pueda verificar que los mensajes hayan sido descargados por el receptor, de esta forma, el emisor del mensaje podrá estar seguro que el destinatario ha recibido su mensaje.

Se puede trabajar sobre una funcionalidad de respuesta rápida para los mensajes recibidos, en donde el usuario destino pueda responder respecto al mensaje enviado por el emisor sin la necesidad de repetir el proceso normal de envío de documentos.

Para evitar la exposición de documentos descifrados por parte de un usuario que haya descargado previamente el documento que le era correspondiente, se puede buscar alternativas que permitan reemplazar el proceso de descarga del documento por un proceso de visualización online del documento, el cual pueda permitirle al usuario ver los documentos que ha recibido y responderlos, la inclusión de este proceso a futuro mejoraría notoriamente la seguridad de información manejada solucionando el problema de la exposición de la información previamente descargada.

BIBLIOGRAFIA

ALCADIA DE BOGOTA. Decreto 1747 de 2000 [En línea] http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277> [citado en 21 de febrero de 2014]

ANDI. Consumo aparente Primer semestre de 2012 [En línea] <http://www.andi.com.co/Archivos/file/Consumo%20aparente%20primer%20semestre%20%202012.xls> [Citado 20 de agosto de 2013]

BRAVO, Silvana. Estudio comparativo de los algoritmos de cifrado de flujo RC4 A5 y SEAL. [En línea].
<http://delta.cs.cinvestav.mx/~francisco/arith/Flujo.pdf> [Citado en mayo 8 de 2014]

BIZAGI. BPMN (Bussiness Process Model and Notation) [En línea] <http://wiki.bizagi.com/es/index.php?title=BPMN> [Citado en marzo 6 de 2014]

BIZAGI. Conectores canales y artefactos [En línea] <http://wiki.bizagi.com/es/index.php?title=Artefactos_swimlanes_y_Objetos_Conectores#artefactos> [Citado en marzo 6 de 2014]

BLOG SAGE EXPERIENCE. Cómo reducir el uso del papel en el día a día de la empresa. [En línea].
<http://blog.sage.es/innovacion-tecnologia/como-reducir-el-uso-del-papel-en-el-dia-a-dia-de-la-empresa> [Citado en 29 de julio de 2013]

CAMARA DE LA REPÚBLICA DE COLOMBIA. "Guía No 1 BUENAS PRÁCTICAS PARA REDUCIR EL CONSUMO DE PAPEL". [En línea] <http://www.camara.gov.co/portal2011/gestor-documental/doc_download/1880->

CONTRALORÍA DE BOGOTÁ. Conceptos de Firma (Certificado) Digital .[En línea]
<http://sivicof.contraloriabogota.gov.co/stormUser/Documentos/Conceptos%20de%20Firma%20Digital.pdf> [Citado en 28 de agosto de 2013]

DIAN. Mecanismo Digital. [En línea]. <http://www.dian.gov.co/descargas/cartillas/Dian-guiaMecanismosDigitales-V1-04_130208.pdf> [Citado en 27 de febrero de 2014]

EROSKI CONSUMER. La firma electrónica [En línea]. <http://www.consumer.es/web/es/tecnologia/internet/2005/02/13/117226.php#> [Citado en 5 de octubre de 2013]

INFORMATION SECURITY. After how much data encryption (AES-256) we should change key? [En línea]. <http://security.stackexchange.com/questions/30170/after-how-much-data-encryption-aes-256-we-should-change-key> [Citado en 6 de mayo de 2014]

LONES, Michael. Encrypting files with public key encryption in Java [En línea]. <http://www.macs.hw.ac.uk/~ml355/lore/pkencryption.htm> [Citado en 25 de septiembre de 2013]

MODELO FACTURA. Firma digital avanzada [En línea]. <http://www.modelofactura.net/firma-digital-avanzada.html> [Citado en 5 de octubre de 2013]

MODELO FACTURA. Firma Digital Reconocida. [En línea] <http://www.modelofactura.net/firma-digital-reconocida.html> [Citado en 5 de octubre de 2013]

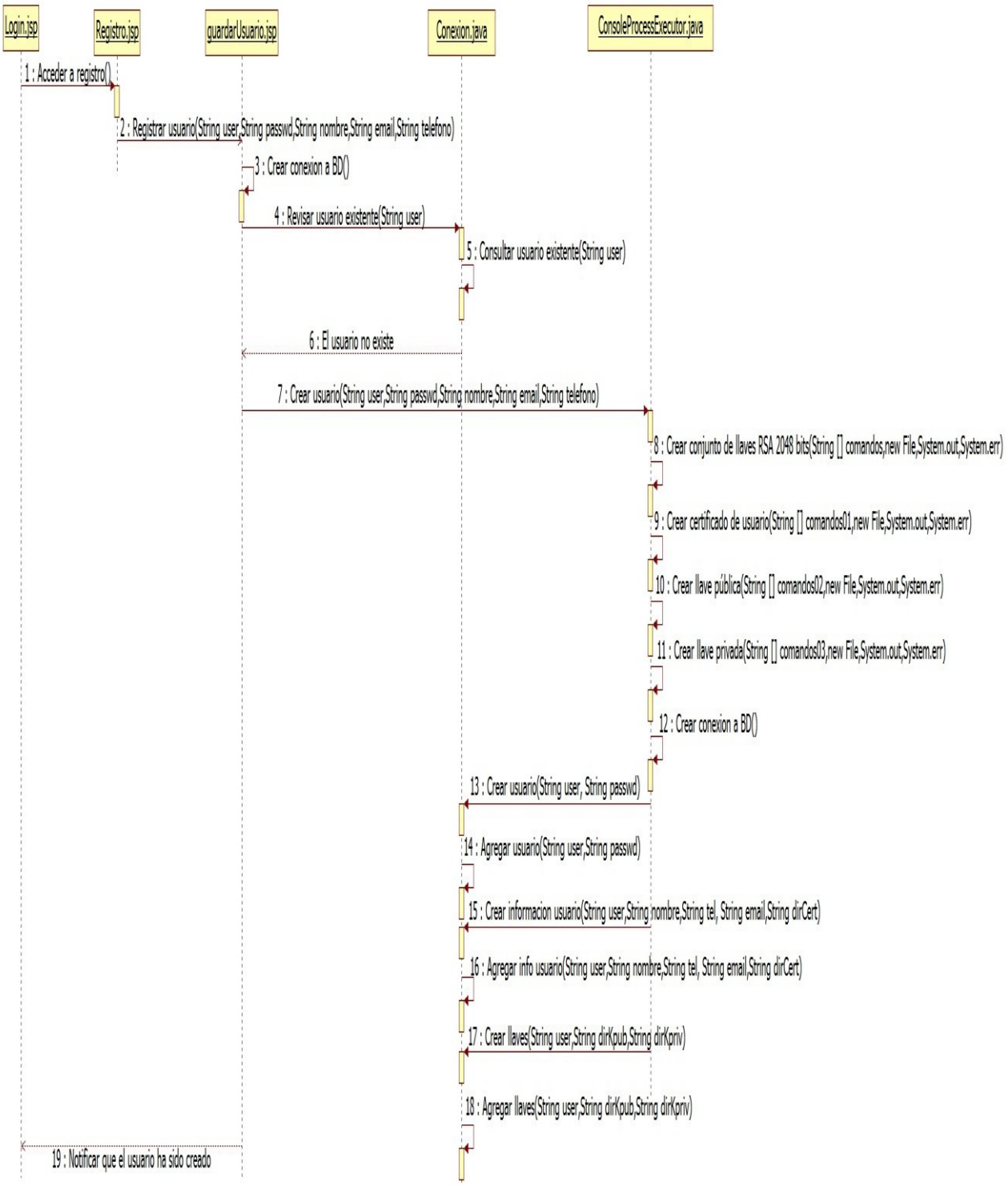
PALANISISAMY V, JENEBA MARY. Hybrid cryptography by the implementation of RSA and AES En: International journal of current research [En línea] (Abril del 2011) <http://www.journalcra.com/sites/default/files/Download%20546.pdf> [Citado en 8 de mayo de 2014]

PENALVA, Cristóbal. Seguridad:Criptografía. [En línea] <http://www.uv.es/montanan/redes/trabajos/criptografia.doc> [Citado en 28 de agosto de 2013]

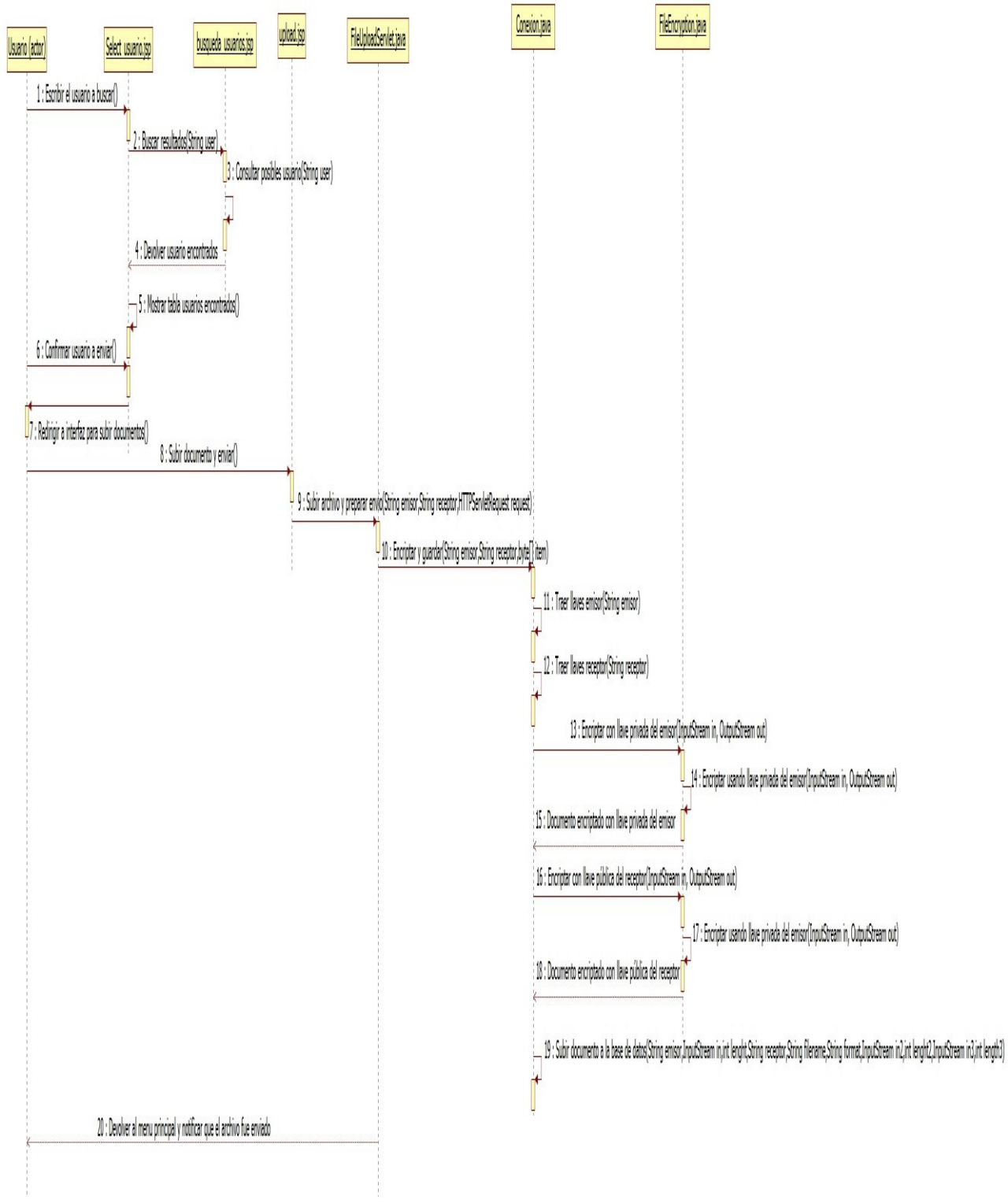
ZONATIC. Sistemas actuales de autentificación y firma [En línea] <http://zonatic.usatudni.es/es/aprendizaje/aprende-sobre-el-dnie/57-aspectos-tecnicos/208-sistemas-actuales-de-autenticacion-y-firma.html> [Citado en 24 de septiembre de 2013]

ANEXOS

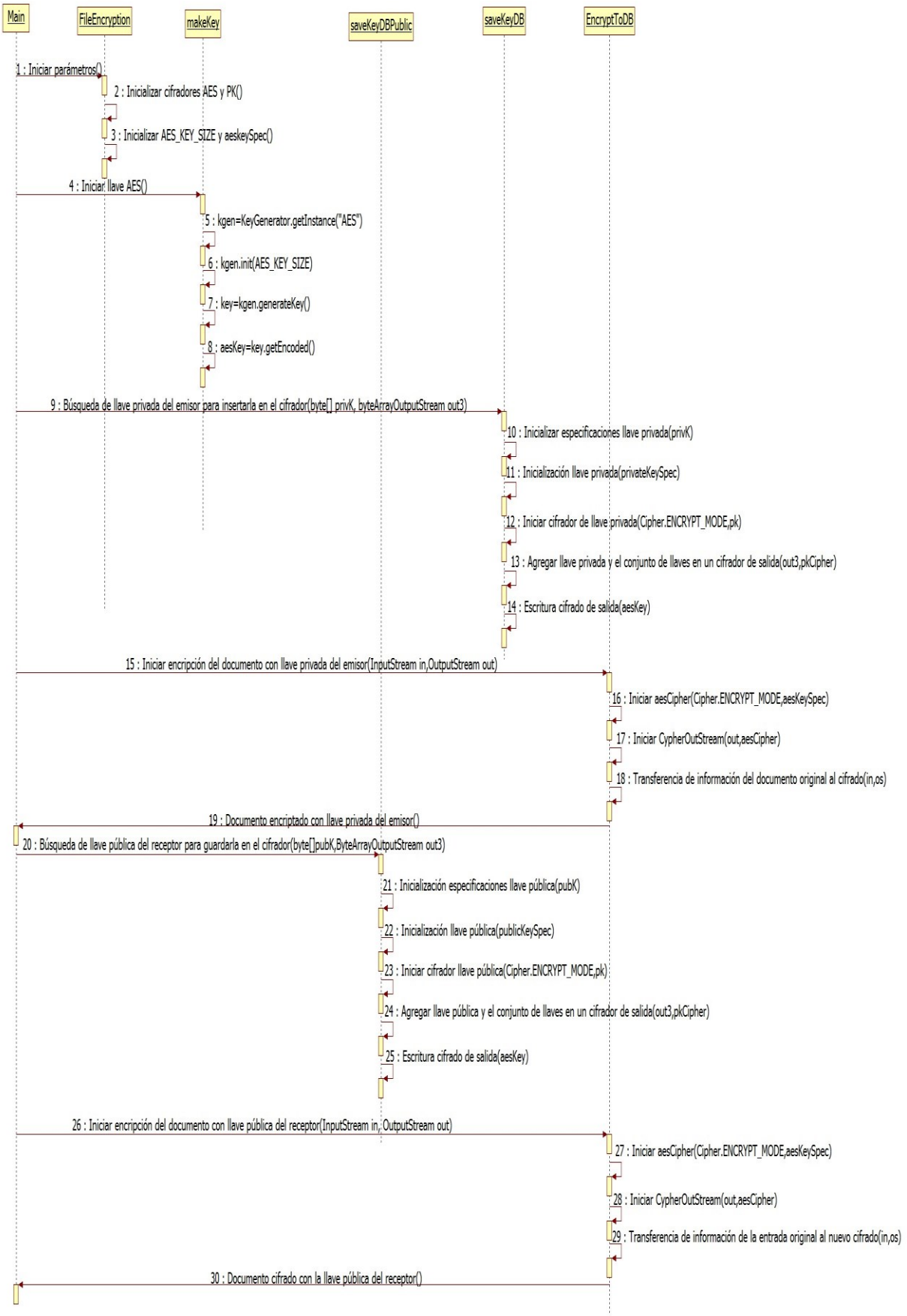
Anexo A. Diagrama de secuencia para el registro de usuario y creación de llaves respectivas



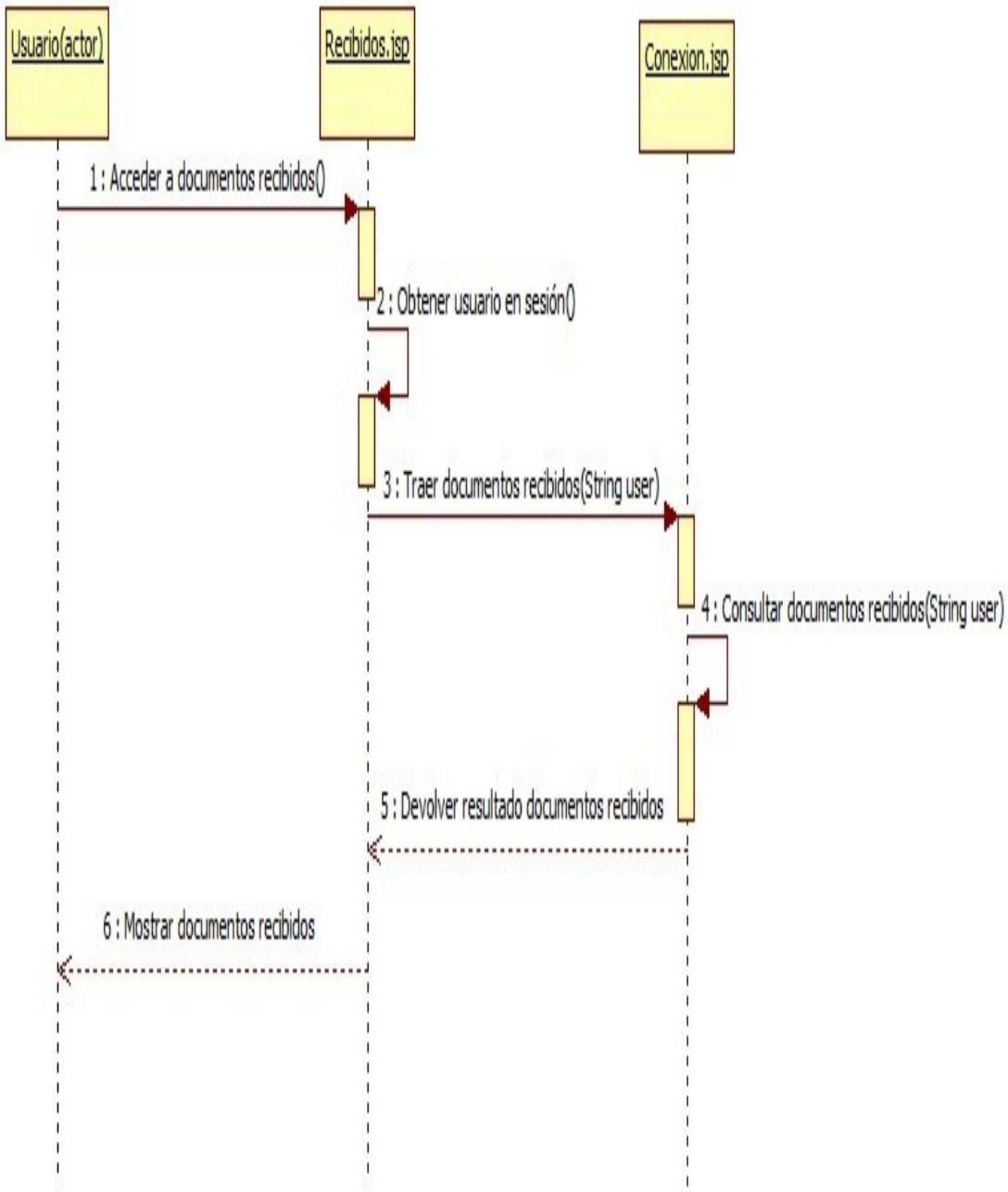
Anexo B. Diagrama de secuencia que explica el proceso de envío de documentos



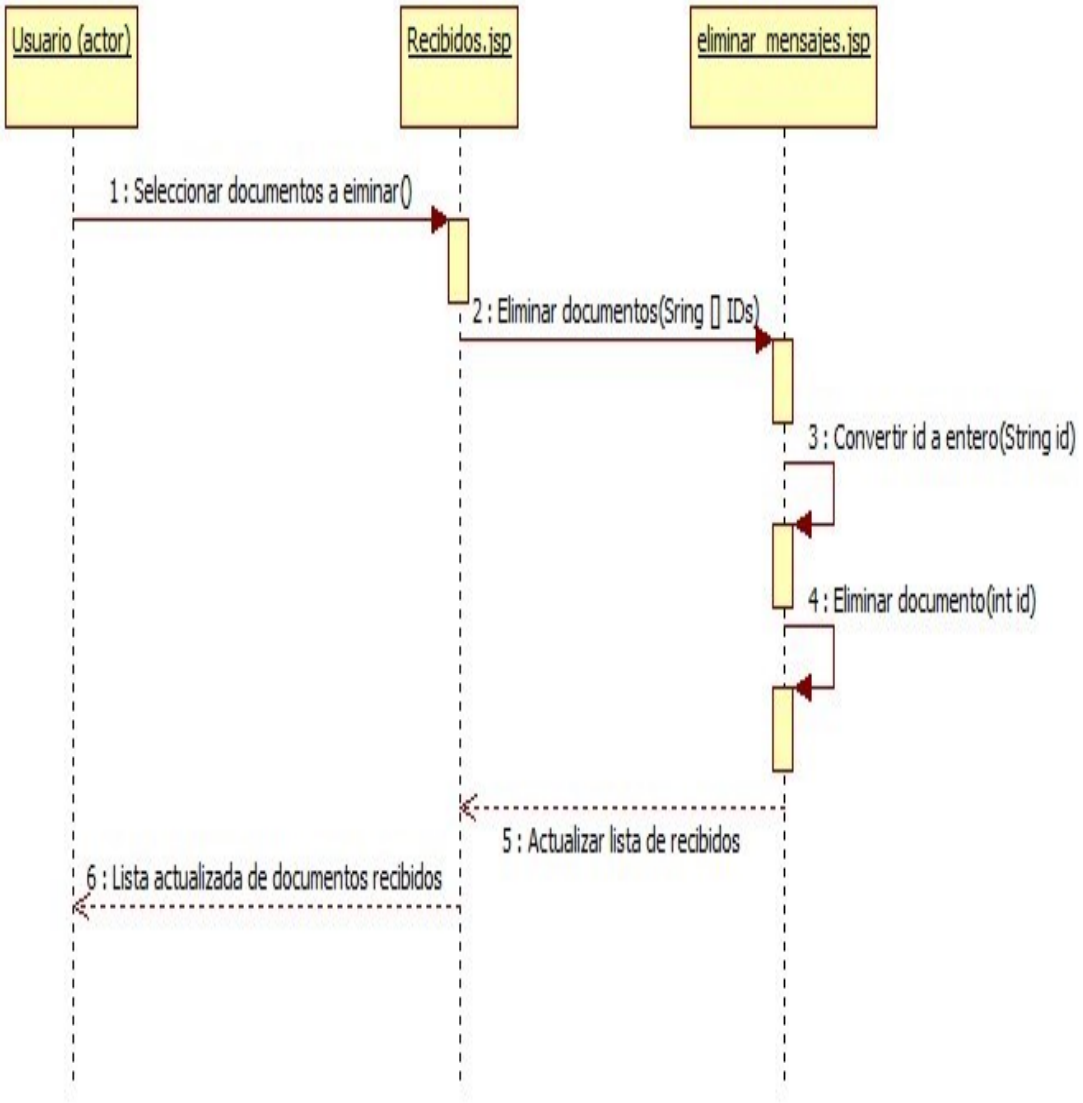
Anexo C. Diagrama de secuencia para la encripción de un documento



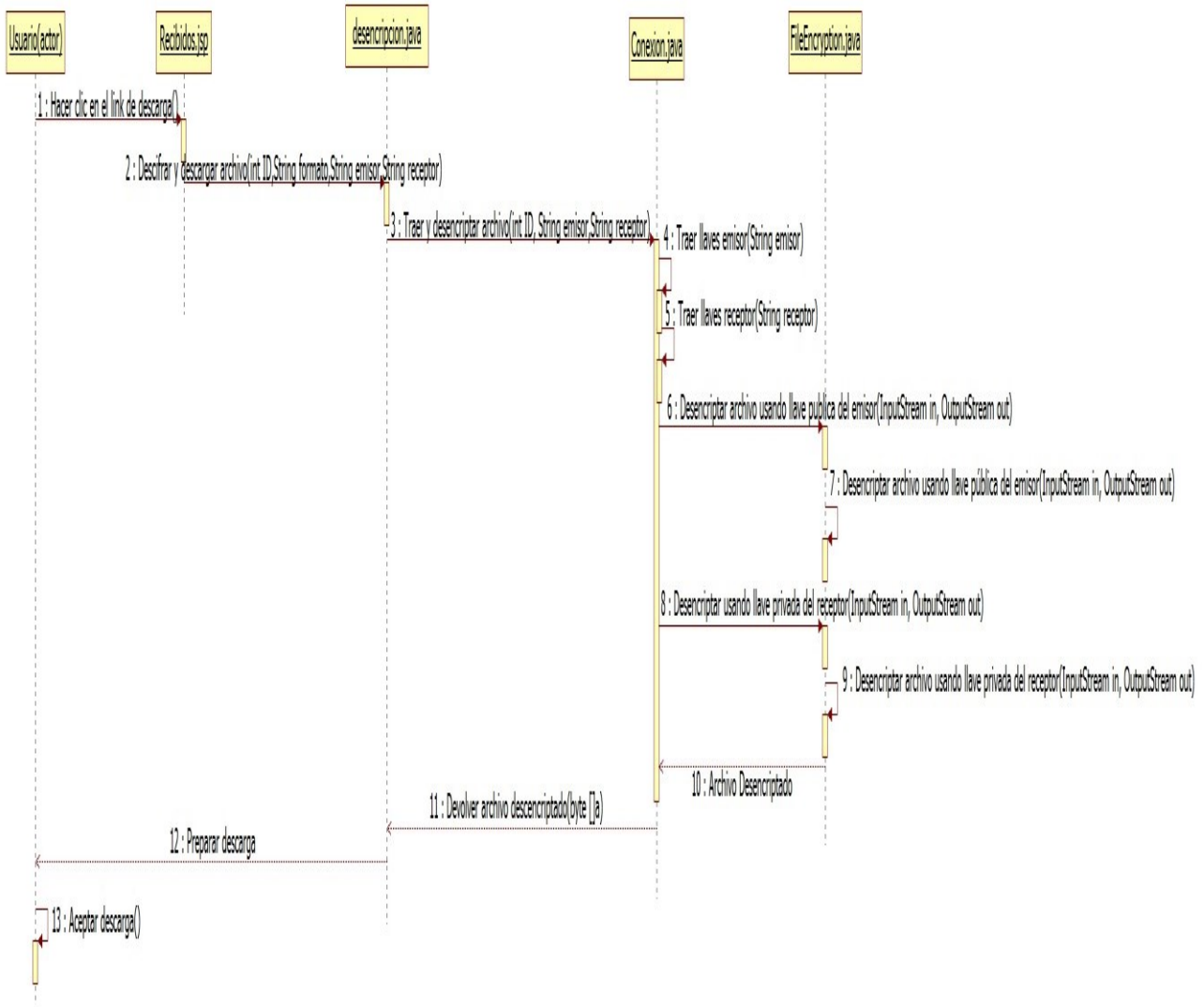
Anexo D. Diagrama de secuencia que explica el proceso de mostrar los documentos recibidos por un usuario



Anexo E. Diagrama de secuencia que explica el proceso de borrado de documentos recibidos por un usuario.



Anexo F. Diagrama de secuencia que explica el proceso de descarga de documentos



Anexo G Diagrama de secuencia que explica el proceso de desencripción de un documento