INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

SEMINARIO DE TITULACIÓN
"SEGURIDAD DE LA INFORMACIÓN"

TESINA

"DISEÑO DE UN SISTEMA DE INFORMACIÓN PARA LA GESTION DE MEMORANDUMS ELECTRÓNICOS EN LA ESIME CULHUACAN"

QUE PRESENTAN PARA OBTENER EL TÍTULO DE
LICENCIADO EN CIENCIAS DE LA INFORMÁTICA

JURADO PADILLA MARÍA DEL PILAR
MARTÍNEZ CABAÑAS KARINA
SALAS BOCANEGRA ELVIA

Asesor:

DR. MOISÉS SALINAS ROSALES

VIGENCIA: DES/ESIME-CUL-2008/23/2/10

Mexico, D.F., Octubre 2010

IPN
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN

TESINA

POR LA OPCIÓN DE TITULACIÓN SEMINARIO EN SEGURIDAD DE LA INFORMACIÓN

QUE PARA OBTENER EL TÍTULO DE LICENCIADO EN CIENCIAS DE LA INFORMÁTICA

DEBERÁN DESARROLLAR:

JURADO PADILLA MARÍA DEL PILAR
MARTÍNEZ CABAÑAS KARINA
SALAS BOCANEGRA ELVIA

"DISEÑO DE UN SISTEMA DE INFORMACIÓN PARA LA GESTION DE MEMORANDUMS ELECTRÓNICOS EN LA ESIME CULHUACAN"

INTRODUCCIÓN

EN LA ACTUALIDAD LA INFORMACIÓN BRINDA GRAN PODER Y RESPONSABILIDAD A QUIEN LA POSEE, ES POR ESO QUE CON FRECUENCIA LAS ORGANIZACIONES E INSTITUCIONES SE ENFRENTAN A PROBLEMAS RELACIONADOS CON LA GESTIÓN Y SEGURIDAD DE LA MISMA, EN MUCHAS DE ELLAS SE REALIZA EL PROCESO DE GESTIÓN DE DOCUMENTOS (MEMORÁNDUMS) FORMA MANUAL, TENIENDO COMO RESULTADO UN GRAN VOLUMEN FÍSICO DE DOCUMENTOS, LO QUE CONLLEVA A UNA CONSULTA TARDÍA, POCO EFECTIVA E INEXACTA. PARA DARLE SOLUCIÓN A ESTE PROBLEMA SE PLANTEA EL DISEÑO DE UN SISTEMA DE INFORMACIÓN ELECTRÓNICO, CON LAS MEJORES MEDIDAS DE SEGURIDAD, PARA GARANTIZAR LA CONFIDENCIALIDAD, INTEGRIDAD Y AUTENTICACIÓN DE LA INFORMACIÓN CONTENIDA EN LOS MEMORÁNDUMS.

CAPITULADO

México D.F., Octubre de 2010

VIGENCIA: DES/ESIME-CUL-2008/23/2/10

DR. GABRIEL SÁNCHEZ PÉREZ
Coordinador del Seminario

DR. MOISÉS SALINAS ROSALES
Asesor

M. EN C. LUIS CARLOS CASTRO MADRID
Jefe de la carrera de I.C.

Agradecimientos

A mis padres:

Antes que nada a ellos por darme la vida, por apoyarme en todos mis proyectos, brindarme toda su comprensión y amor porque sin ello, no hubiera alcanzado esta meta más en mi vida. Y aunque mi padre ya no esté conmigo físicamente yo se que se sentirá muy orgulloso, ya que este logro no solo es mío si no suyo también.

Gracias padre por tus enseñanzas y a ti madre por tus fortalezas.

A mis hermanas:

Que siempre me han apoyado y han estado a mi lado, brindándome sus consejos y comprensión.

Pilar Jurado Padilla

Agradecimientos

Agradezco a todos los amigos y compañeros que me han apoyado a lo largo de este tiempo.

Gracias al Doctor Moisés, por brindarnos su paciencia, tiempo, atención y dedicación durante el desarrollo de este trabajo.

Especialmente gracias a Yolanda, Ismael, Erika, Berenice y Miguel Ángel que siempre han estado conmigo en las buenas y en las malas, porque somos familia.

Daniel Pacheco, gracias por encaminarme nuevamente a terminar con lo que hace mucho comencé, gracias por tu apoyo, por recordarme que puedo cumplir mis propósitos, por ser paciente, insistente y comprensivo.

A todos, ¡Gracias!

Karina Martínez Cabañas

Agradecimientos

A mis padres, les agradezco infinitamente por todo el apoyo que me brindaron durante el desarrollo de mi carrera, por la educación y los valores que me inculcaron, quiero que sepan que su amor, comprensión y apoyo, fueron la base fundamental para sentirme inspirada a terminar con esta meta en mi vida.

A mi esposo, le agradezco principalmente el amor que me demostro durante este trayecto profesional, por todo su apoyo paciencia y tolerancia, además de que le doy gracias a dios por darme la dicha de que mi esposo este vivo y comparta este momento conmigo.

También le doy gracias a esa personita que siempre estuvo conmigo durante esta ultima fase en mi proceso de titulación y que compartió conmigo preocupaciones, tristezas, angustias y principalmente mucha alegría, y que aunque aun no me lo puede decir, se que le da mucho gusto y que esta feliz, el es mi hijo Danielito.

Elvia Salas Bocanegra.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

CAPÍTULO I

ANTECEDENTES

1.1 Introducción

En la actualidad la información brinda gran poder y responsabilidad a quien la posee, es por eso que con frecuencia las organizaciones se enfrentan a problemas relacionados con la gestión y seguridad de la información, los cuales pueden generar pérdidas cuantiosas y en ocasiones su desaparición.

La creación de documentos (memorándums) así como el archivado de los mismos, es una tarea que desarrollan todas las organizaciones e instituciones, en muchas de ellas el manejo, archivado, y elaboración de memorándums, se realiza de forma manual, teniendo como resultado un gran volumen físico de documentos, lo que conlleva a una consulta tardía, poco efectiva e inexacta.

La gestión de esta información es una tarea que conlleva a una gran responsabilidad, principalmente debido al acceso no autorizado a ella, lo cual implica la manipulación por parte de personas ajenas, utilizándola a favor, por ejemplo: ofreciéndola al mejor postor.

Para enfrentar este problema existen diferentes mecanismos de solución, en el presente trabajo, se plantea la solución al mismo mediante un sistema de información electrónico, con las mejores medidas de seguridad, para garantizar la confidencialidad, integridad y autenticación de la información contenida en los memorándums. Dicha solución se desarrolla en cuatro capítulos descritos a continuación:

En el Capítulo I se desarrollan los antecedentes de nuestro trabajo como son, la problemática a solucionar, la introducción al tema, justificación del mismo y los conceptos básicos para la comprensión del desarrollo.

Durante el Capítulo II se describen precisamente las herramientas y metodología a utilizar para el desarrollo del diseño, se presenta la justificación y ventajas del uso de cada uno de ellas.

Es importante mencionar que el objetivo de los dos siguientes capítulos es entregar un diseño de sistema orientado a objetos, basado en el análisis del problema y requerimientos, implementando mecanismos de seguridad que garanticen la misma en el sistema.

En el Capítulo III se desarrolla la investigación y comprensión de los requisitos, la cual representa el desarrollo de la investigación para la determinación de los requisitos funcionales y no funcionales, sobre los cuales se basa el resto del trabajo, ya que de estos se obtienen los casos de uso y la arquitectura de dicho sistema, así como la comprensión del negocio y el proceso de gestión de memorándums.

Por último el Capítulo IV se desarrolla la extracción de los diagramas de clases, diagramas de secuencia y la arquitectura del sistema.

1.2 Planteamiento Del Problema

En la ESIME Culhuacan no se cuenta con un sistema de gestión de documentos (memorándums) electronicos, el principal problema radica en la falta de infraestructura tecnológica, para dicho proceso.

En la actualidad el personal lleva a cabo el proceso de gestión de memorándums de forma manual, lo cual genera que este sea poco seguro y eficaz.

1.3 Objetivos

Objetivo General:

Diseñar un Sistema de Información de Gestión de Memorándums Electrónicos en la ESIME Culhuacan, usando la metodología RUP.

Objetivos Particulares:

- Identificar y comprender los requerimientos para el procesamiento de memorándums en formato electrónico dentro de la ESIME Culhuacan.
- Comprender y aplicar la metodología de desarrollo RUP y la herramienta de modelo UML.
- Seleccionar las herramientas criptográficas acordes a las necesidades de seguridad de información del sistema.
- Proponer una arquitectura general de sistema (proponer módulos y especificar que hace cada una de ellas y como es su interrelación)

1.4 Justificación

El uso de procesos y métodos seguros en las organizaciones han llevado al diseño, desarrollo y aplicación de herramientas que los garanticen, de tal forma que sean confiables y de fácil uso.

Así mismo, el uso de recursos naturales hoy en día ha tomado gran importancia en los ámbitos social, económico y ecológico. Dando como consecuencia el ahorro de los mismos en todas las organizaciones.

Tomando en cuenta lo complejo que actualmente es administrar la información decidimos desarrollar este proyecto con la finalidad de automatizar el acceso a la información a si como la dispersion de la misma, garantizando que los procesos internos, en particular la emisión consulta y búsqueda de memorándums de la ESIME Culhuacan sean seguros y ayuden a optimizar el ahorro del papel.

1.5 Alcances

Para el desarrollo de esta tesina se plantean los siguientes alcances:

Elaborar propiamente un diseño para la creación de un Sistema de información de gestión de memorándums electrónicos, para la ESIME Culhuacan, utilizando la metodología RUP así como el lenguaje UML a su vez, recomendando las herramientas criptográficas que fueron analizadas con anterioridad por el Ingeniero Especialista Simon Pedro Torres en la tesis firma digital 2009.

El proyecto consiste en desarrollar un diseño para un sistema, con el cual un usuario sea capaz de gestionar memorándums electrónicos mediante el uso de un método seguro, que permita agilizar tanto el acceso como garantizar la autenticidad y la recuperación de memorándum almacenados.

1.6 Sistema De Información

Un sistema de información (SI) es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (objetivo). [1]

Dichos elementos formarán parte de alguna de estas categorías:

Elementos de un sistema de información (figura 1.1).

- Personas.
- Datos.
- Actividades o técnicas de trabajo.
- Recursos materiales en general (típicamente recursos informáticos y de comunicación, aunque no tienen por qué ser de este tipo obligatoriamente).

En la figura 1.1, se muestra como todos estos elementos interactúan entre sí para procesar los datos (incluyendo procesos manuales y automáticos) dando lugar a información más elaborada y distribuyéndola de la manera más adecuada posible en una determinada organización en función de sus objetivos.

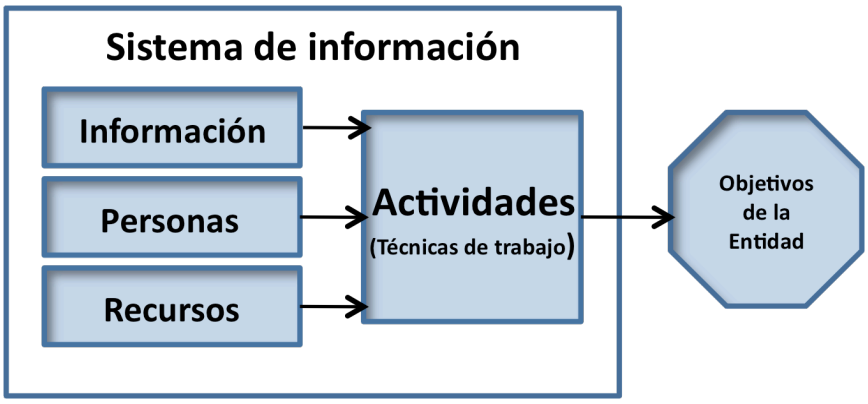

Figura 1.1 Sistema de Información

Además recopila, manipula, almacena y crea reportes de información respecto de las actividades de negocios de una empresa, con el fin de ayudar a la administración de la misma en el manejo de operaciones de negocio.

1.7 Memorándums

La palabra "memorándum" proviene del latín. Significa "algo que hay que recordarse". Se refiere a una nota escrita, menos formal que una carta.

Es aquel escrito que se usa para intercambiar información entre diferentes departamentos de una empresa, con el propósito de dar a conocer alguna recomendación, indicación, instrucción, disposición, etc. [2]

Generalmente este tipo de escrito contiene las siguientes partes:

- El nombre de la persona a quien va dirigido.
- El nombre del remitente.
- La fecha.
- El asunto.
- El texto.
- La firma del remitente.

Su redacción debe ser breve, clara y precisa; aún cuando en este tipo de comunicación no se acostumbra usar la despedida, hay ocasiones en que se debe utilizar para darle un toque personal y cortés al mensaje.

1.8 Sistema de Gestión de Memorándums Electrónicos.

Un Sistema de Gestión de Memorándums, se puede entender como un programa informático utilizado para rastrear y archivar documentos electrónicos. Hay varias cuestiones comunes vinculadas a la gestión de documentos, tanto si es un sistema informal, o un método basado en papel para una persona, como si es formal, estructurado, elaborado por computadora para muchas personas de muchas oficinas.[3],[4]

Para efectos de este trabajo se descartan todos los documentos y se plasma que cuando hagamos mención de ellos, nos referimos específicamente a memorándums.

La mayoría de los métodos de gestión de documentos tienen las siguientes áreas:
Almacenamiento: ¿Dónde se archivarán los documentos?

Llenado: ¿Cómo serán llenados los documentos? ¿Qué métodos serán utilizados para organizar o indexar los documentos y permitir su acceso posterior? ***Recuperación***: ¿Cómo serán encontrados los documentos? En general la recuperación se relaciona con la navegación a través de los documentos y la recuperación de cierta información específica.

Seguridad: ¿Cómo serán protegidos los documentos? ¿Cómo el personal no autorizado será imposibilitado de ver, modificar o destruir los documentos?

Recuperación tras desastres: ¿Cómo pueden los documentos ser recuperados en caso de destrucción por incendios, inundaciones o desastres naturales?

Período de retención: ¿Cuánto tiempo deberían los documentos ser guardados?

Distribución: ¿Cómo pueden los documentos estar disponibles para la gente que los necesita?

Flujo de trabajo: Si los documentos necesitan pasar de una persona a otra, ¿cuáles son las reglas respecto a cómo su trabajo debería fluir?

Autenticación: ¿Hay alguna forma de asegurad la autenticidad de un documento?

CAPÍTULO II

HERRAMIENTAS PARA EL DISEÑO DEL SISTEMA DE INFORMACIÓN

En este capítulo se describen las principales características de las herramientas que se emplearán para la elaboración del diseño del sistema de gestión de memorándums electrónicos.

2.1 RUP

El Proceso Unificado Racional (*Rational Unified Process* RUP), es un proceso de desarrollo de software y junto con el Lenguaje Unificado de Modelado UML, constituye la metodología estándar más utilizada para el análisis, implementación y documentación de sistemas orientados a objetos.

El RUP no es un sistema con pasos firmemente establecidos, sino un conjunto de metodologías adaptables al contexto y necesidades de cada organización

2.1.1 Orígenes.

El antecedente más importante se ubica en 1967 con la Metodología Ericsson (Ericsson Approach) elaborada por Ivar Jacobson, una aproximación de desarrollo basada en componentes, que introdujo el concepto de Caso de Uso. Entre los años de 1987 a 1995 Jacobson fundó la compañía Objectory AB y lanza el proceso de desarrollo Objectory (abreviación de Object Factory).

Posteriormente en 1995 Rational Software Corporation adquiere Objectory AB y entre 1995 y 1997 se desarrolla Rational Objectory Process (ROP) a partir de Objectory 3.8 y del Enfoque Rational (Rational Approach) adoptando UML como lenguaje de modelado.

Desde ese entonces y a la cabeza de Grady Booch, Ivar Jacobson y James Rumbaugh, Rational Software desarrolló e incorporó diversos elementos para expandir ROP, destacándose especialmente el flujo de trabajo conocido como modelado del negocio. En junio del 1998 se lanza Rational Unified Process RUP. [5]

2.1.2 Descripción del Proceso

La metodología de Proceso Unificado como ya se mencionó surge del paradigma orientado a objetos, el Proceso Unificado es más que una serie de pasos que si se sigue, resultaran en la construcción de un sistema informático, basado en 3 características esenciales:

- **Los Casos de Uso:** son una técnica de captura de requisitos que fuerza a pensar en términos de importancia para el usuario y no sólo en términos de funciones que sería bueno contemplar. Los Casos de Uso representan los requisitos funcionales del sistema.
  En RUP los Casos de Uso no son sólo una herramienta para especificar los requisitos del sistema. También guían su diseño, implementación y prueba.

- **Proceso centrado en la arquitectura:** la arquitectura de un sistema es la organización o estructura de sus partes más relevantes, lo que permite tener una visión común entre todos los involucrados (desarrolladores y usuarios) y una perspectiva clara del sistema completo, necesaria para controlar el desarrollo. La arquitectura involucra los aspectos estáticos y dinámicos más significativos del sistema, está relacionada con la toma de decisiones que indican cómo tiene que ser construido el sistema y ayuda a determinar en qué orden. Además la definición de la arquitectura debe tomar en consideración elementos de calidad del sistema, rendimiento, reutilización y capacidad de evolución por lo que debe ser flexible durante todo el proceso de desarrollo.

  La arquitectura se ve influenciada por la plataforma software, sistema operativo, gestor de bases de datos, protocolos, consideraciones de desarrollo como sistemas heredados. Muchas de estas restricciones constituyen requisitos no funcionales del sistema.

- **Proceso iterativo e incremental:** es en donde el trabajo se divide en partes más pequeñas o mini proyectos. Cada mini proyecto se puede ver como una iteración, del cual se obtiene un incremento que produce un crecimiento en el producto. En la figura 2.1 se muestra como una iteración puede realizarse por medio de una cascada. Se pasa por los flujos fundamentales (Requisitos, Análisis, Diseño, Implementación y Pruebas) también existe una planificación de la iteración, un análisis de la iteración y algunas actividades específicas de la iteración.

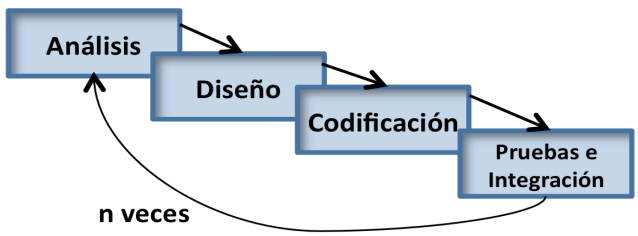

Figura 2.1 Proceso iterativo e incremental

2.1.3 Dimensiones de RUP

El proceso puede ser descrito en dos dimensiones o ejes:

- **Eje horizontal**: Representa el tiempo y es considerado el eje de los aspectos dinámicos del proceso. Indica las características del ciclo de vida del proceso expresado en términos de fases, iteraciones e hitos. En la Figura 2.2 se puede observar que RUP consta de cuatro fases: Inicio, Elaboración, Construcción y Transición y cada fase se subdivide a la vez en iteraciones
- **Eje vertical:** Representa los aspectos estáticos del proceso. Describe el proceso en términos de componentes de proceso, disciplinas, flujos de trabajo (Workflow), actividades, artefactos y roles.

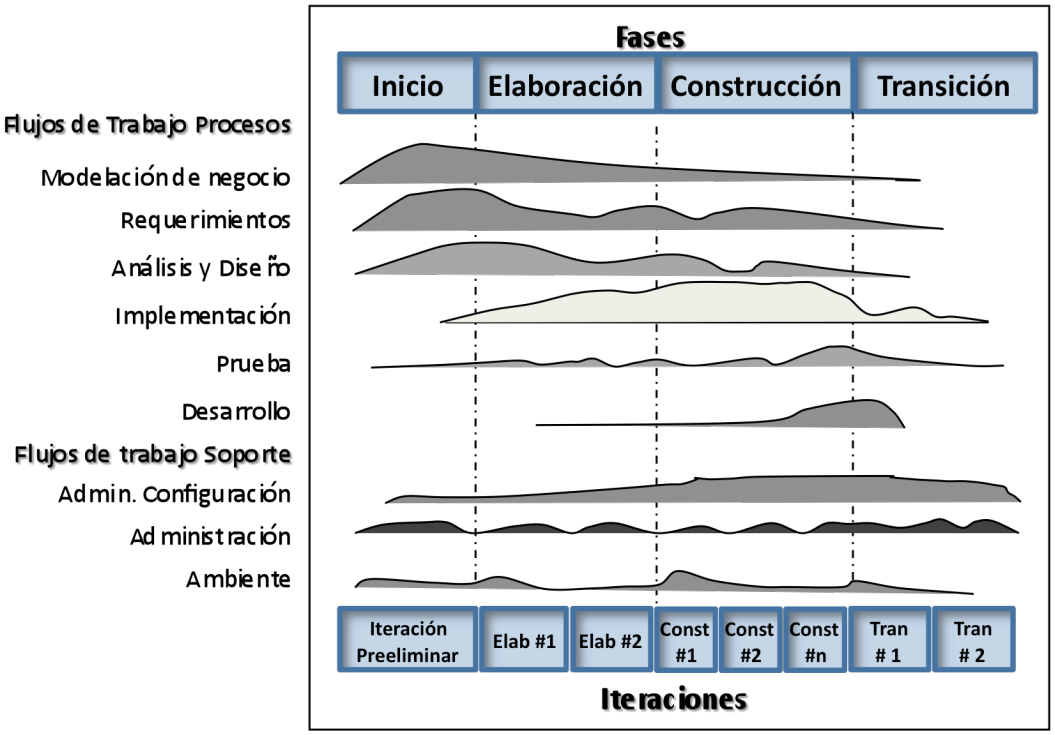

Figura 2.2 Diagrama de Flujos de trabajo y fases del proceso unificado

2.1.4 Fases

El ciclo de vida consiste en una serie de ciclos, cada uno de los cuales produce una nueva versión del producto, véase figura 2.3, cada ciclo está compuesto por fases y cada una de estas fases está compuesta por un número de iteraciones: [6]

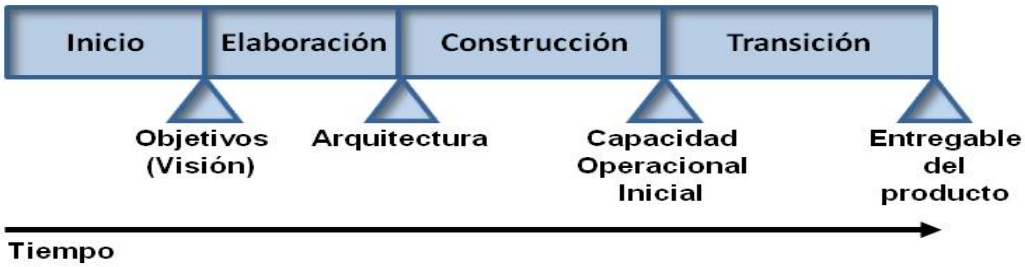

Figura 2.3 Transición

- **Inicio.-** Define el ámbito y objetivos del proyecto. En él se define la funcionalidad y capacidades del producto, es decir; su objetivo principal es determinar si el sistema de información es económicamente viable.
- **Elaboración.-** Tanto la funcionalidad como el dominio del problema se estudian en profundidad. Se define una arquitectura básica y se planifica el proyecto considerando recursos disponibles.
- **Construcción.-** El producto se desarrolla a través de iteraciones donde cada iteración involucra tareas de análisis, diseño e implementación. Las fases de estudio y análisis sólo dieron una arquitectura básica que es aquí refinada de manera incremental conforme se construye (se permiten cambios en la estructura).

  En esta fase se realiza gran parte del trabajo es programación y pruebas así como la documentación tanto del sistema construido como del manejo del mismo.

- **Transición.-** Se libera el producto y se entrega al usuario para un uso real. Se incluyen tareas de marketing, empaquetado atractivo, instalación, configuración, entrenamiento, soporte, mantenimiento, etc.
  Los manuales de usuario se completan y refinan con la información anterior.
  Estas tareas se realizan también en iteraciones. Todas las fases no son idénticas en términos de tiempo y esfuerzo.

La figura 2.4 muestra una descripción general de las actividades realizadas dentro de cada intersección (fases-workflow) del proceso unificado, con la finalidad de lograr un mejor entendimiento de dicha metodología.

	Inicio	Elaboración	Construcción	Transición
Workflow de los requisitos	Se determina si el sistema de información propuesto es económicamente viable. Se determinan los requisitos iniciales	Se refinan los requisitos iniciales.	Se verifican los requisitos, si se detecta alguna falla o cambio.	Se asegura que los requisitos del cliente se hayan cumplido
Workflow del análisis	Análisis de algunos casos de uso críticos.	Se entrega el modelo de negocios terminado.	Si se detecta alguna falla o cambio, se vuelve a revisar el modelo de negocios.	Se realizan los cambios, si hay alguna falla o cambio que involucre el análisis.
Workflow del diseño	Comienza diseño de la arquitectura basado en el análisis de casos críticos.	Se realiza el refinamiento de la arquitectura básica.	Se entrega una arquitectura terminada.	Se realizan los cambios, si hay alguna falla o cambio que involucre el diseño.
Workflow de la implementación	Con frecuencia no se realiza ninguna codificación, en ocasiones, se realiza un prototipo de pruebas de concepto, para probar la viabilidad del sistema propuesto.	Se entrega un plan de administración del proyecto.	Se produce una versión Beta del sistema de información.	Se corrigen las fallas del sistema de información. Se entrega el producto final.
Workflow de pruebas	El objetivo es asegurar que los requisitos se hayan determinado con precisión.	Se genera un caso de negocio terminado.	Pruebas de la versión beta, pruebas de integración de modulos	Se realizan pruebas de calidad.
	Iteración Preeliminar	Elab #1	Elab #2	Const #1	Const #2	Const #N	Tran # 1	Tran # 2

Figura 2.4 Descripción de Actividades por Intersección.

2.1.5 Ventajas contra otras metodologías

Existen varias ventajas sobre otras metodologías:

- La principal ventaja es que RUP se basa en pruebas realizadas en campo, ya que es un proceso de desarrollo general.
- Se basa también en Casos de Uso para describir lo que se tiene y lo que se espera del software.
- El proceso unificado es una metodología iterativa y por incrementos.
- Se documenta de la mejor manera basándose en UML (Unified Modeling Language - Lenguage de Modelado Unificado).
- Es una metodología para sistemas de duración extendida.
- Se pueden detectar problemas y fallas de forma temprana.

2.1.6 Justificación del uso de RUP

Es una metodología flexible de procesos de desarrollo de software, es decir es una metodología adaptable y estándar que actualmente es la más utilizada para el análisis, implementación y documentación de sistemas orientados a objetos.

RUP describe como utilizar de forma efectiva las reglas de negocio y los procedimientos comerciales. Así como también permite seleccionar el conjunto de componentes de proceso que se ajustan a las necesidades del proyecto.

A continuación se describirá el UML, que es el lenguaje utilizado para la documentación de la metodología RUP.

2.2 Lenguaje Unificado de Modelado (UML)

Desde los inicios de la informática se han estado utilizando distintas formas de representar los diseños de una manera más bien personal o con algún modelo gráfico, La falta de estandarización en la representación gráfica de un modelo impedía que los diseños gráficos realizados se pudieran compartir fácilmente entre distintos diseñadores, con este objetivo se creo el Lenguaje Unificado de Modelado (UML: Unified Modeling Language).

2.2.1 Orígenes

El UML es la creación de Grady Booch, James Rumbaug e Ivar Jacobson. Cada uno de ellos trabajaban en empresas distintas durante la década de los 80´s y a principios de los años 90´s cada uno de ellos diseñó su propia metodología para el análisis y diseño orientado a objetos, posteriormente empezaron a intercambiar ideas de cada una de sus metodologías dándose así la creación de UML. Siendo aceptado rápidamente en la industria del software como el lenguaje gráfico estándar para especificar, construir, visualizar y documentar sistemas con gran cantidad de software.

UML sólo se trata de una notación estándar para el modelado de sistemas de software, es decir, de una serie de reglas y recomendaciones para representar modelos, siendo así el más conocido y utilizado en la actualidad; respaldado por el consorcio OMG (Object Management Group). Es un lenguaje gráfico para visualizar, especificar, construir y documentar un sistema. UML ofrece un estándar para describir un "plano" del sistema (modelo), incluyendo aspectos conceptuales tales como procesos de negocio y funciones del sistema, y aspectos concretos como expresiones de lenguajes de programación, esquemas de bases de datos y componentes reutilizables.

2.2.2 Descripción del lenguaje

UML (unified modeling lenguaje) Es un lenguaje estándar para escribir planos de software. UML puede utilizarse para visualizar, especificar, construir y documentar los artefactos de un sistema que involucran gran cantidad de software.

UML es un lenguaje de propósito general para el modelado orientado a objetos, que combina notaciones provenientes desde: Modelado Orientado a Objetos, Modelado de Datos, Modelado de Componentes, Modelado de Flujos de Trabajo (*Workflows*).

En todos los ámbitos de la ingeniería se construyen modelos, en simplificaciones de la realidad, para poder comprender mejor el sistema que vamos a desarrollar: los arquitectos utilizan y construyen planos (modelos) de los edificios, los grandes diseñadores de coches preparan modelos en sistemas existentes con todos los detalles y los ingenieros de *software* deberían igualmente construir modelos de los sistemas *software*, es para ello que utilizamos UML

2.2.3 Descripción de los diagramas

Un modelo captura una vista de un sistema del mundo real. Es una abstracción de dicho sistema, considerando un cierto propósito. Así, el modelo describe completamente aquellos aspectos del sistema que son relevantes al propósito del modelo, y a un apropiado nivel de detalle.

Un diagrama es una representación gráfica de una colección de elementos de modelado, a menudo dibujada como un grafo conexo de nodos (elementos) y arcos (relaciones).

Un proceso de desarrollo de *software* debe ofrecer un conjunto de modelos que permitan expresar el producto desde cada una de las perspectivas de

interés. Es aquí donde se hace evidente la importancia de UML en el contexto de un proceso de desarrollo de software.

Cada modelo es completo desde su punto de vista del sistema, sin embargo, existen relaciones de enlaces entre los diferentes modelos.

Varios modelos aportan diferentes vistas de un sistema los cuales nos ayudan a comprenderlo desde varios frentes. Así, UML recomienda la utilización de nueve diagramas, para representar las distintas vistas de un sistema como se muestra en la figura 2.5.

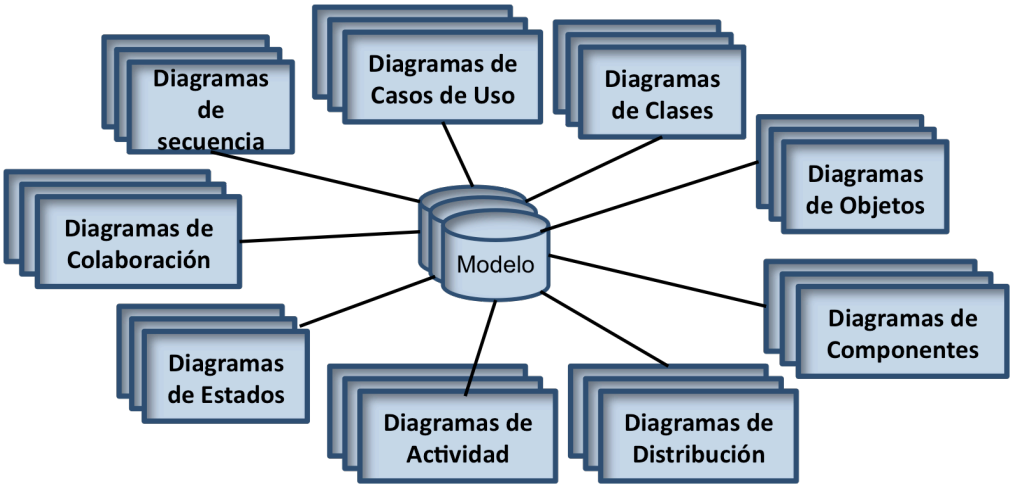

Figura 2.5 Diagramas partes de un modelo

Diagramas Estructurales: Los cuatro diagramas estructurales de UML existen para visualizar, especificar, construir y documentar los aspectos estáticos de un sistema. Se pueden ver los aspectos estáticos de un sistema como aquéllos que representan su esqueleto y su andamiaje, ambos relativamente estables. Los aspectos estáticos de un sistema de software incluyen la existencia y ubicación de clases, interfaces, colaboraciones componentes y nodos.

Los diagramas estructurales de UML se organizan en líneas generales alrededor de los principales grupos de elementos que aparecen al modelar el sistema:

1. Diagramas de clases.	Clases, interfaces y colaboraciones.
2. Diagramas de objetos.	Objetos.
3. Diagramas de componentes.	Componentes.
4. Diagramas de despliegue.	Nodos.

Diagramas de clases: Para poder entender los diagramas de clases, comencemos por explicar que una clase es una categoría o grupo de cosas que tienen atributos y acciones similares. Los diagramas de clases son los diagramas más comunes en el modelado de sistemas orientados a objetos. Estos se utilizan para describir la vista de diseño estática de un sistema. Los diagramas de clases que incluyen clases activas se utilizan para cubrir la vista de procesos estática de un sistema.

En sí, podríamos decir que un diagrama de clases es un tipo de diagrama que nos describe la estructura de un sistema mostrando sus clases (es una categoría o grupo de cosas que tienen atributos y acciones similares), atributos (propiedades o características) y las relaciones entre ellos. Los diagramas de clases son utilizados durante el proceso de análisis y diseño de los sistemas, donde se crea el diseño conceptual de la información que se manejará en el sistema, y los componentes que se encargaran del funcionamiento y la relación entre uno y otro.

Podríamos poner como ejemplo de una clase a las lavadoras, ésta a su vez tiene atributos específicos como pueden ser: la marca, el modelo, número de serie y la capacidad. Entre las acciones de las cosas de esta clase se encuentran “agregar ropa”, “agregar detergente” y “sacar ropa”.

En representación gráfica de este ejemplo de diagramas de clase quedaría como se muestra en la figura 2.6, ya que un rectángulo es el símbolo de la representación de una clase y se divide en tres áreas, donde la parte superior corresponde al nombre de la clase, la parte central a los atributos y la parte inferior a las acciones.

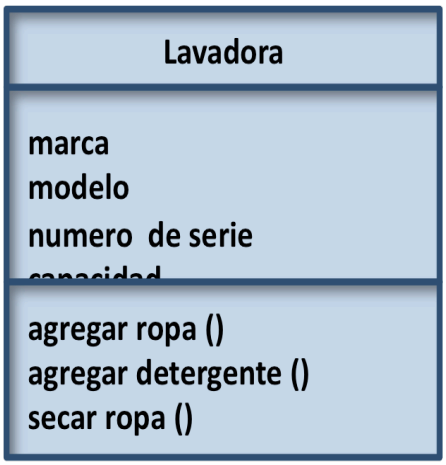

Figura 2.6 Diagramas de clases

Diagramas de objetos. Representa un conjunto de objetos y sus relaciones. Se utilizan para describir estructura de datos, instantáneas de las instancias de los elementos encontrados en los diagramas de clases. Los diagramas de objetos cubren la vista de diseño estática o la vista de procesos estática de un sistema. La forma en que UML representa a un objeto, es en base a un rectángulo como en una clase, pero el nombre está subrayado y el nombre de la instancia específica se encuentra a la izquierda de los dos puntos (:) y el nombre de la clase a la derecha, como se muestra en la figura 2.7.

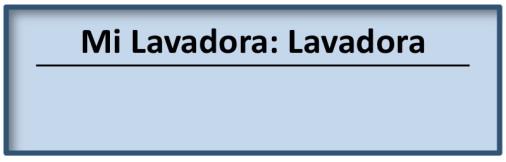

Figura 2.7 Diagramas de objetos

Diagramas de componentes. Muestra un conjunto de componentes y sus relaciones. Los diagramas de componentes se utilizan para describir la vista de implementación estática de un sistema. Los diagramas de componentes se relacionan con los diagramas de clases en que un componente normalmente se corresponde con una o más clases, interfaces o colaboraciones.

En la figura 2.8 Se ilustra cómo es la representación gráfica de un componente en UML.

Figura 2.8 Diagrama de componentes UML

Diagramas de despliegue. Muestra un conjunto de nodos y sus relaciones. Los diagramas de despliegue se utilizan para describir la vista de despliegue estática de una arquitectura. Los diagramas de despliegue se relacionan con los diagramas de componentes en que un nodo normalmente incluye uno o más componentes.

Diagramas de Comportamiento: Los cinco diagramas de comportamiento de UML se emplean para visualizar, especificar, construir y documentar los aspectos dinámicos de un sistema. Se pueden ver los aspectos dinámicos de un sistema como aquéllos que representan sus partes mutables. Los aspectos dinámicos de un sistema de software involucran cosas tales como el flujo de mensajes a lo largo del tiempo y el movimiento físico de componentes en una red.

Los diagramas de comportamiento de UML se organizan en líneas generales alrededor de las formas principales en que se pueden modelar la dinámica de un sistema.

1. Diagramas de casos de uso: Organiza los comportamientos del sistema.
2. Diagramas de secuencia: Centrados en la ordenación temporal de los mensajes.
3. Diagramas de colaboración: Centrados en la organización estructural de los objetos que envían y reciben mensajes.
4. Diagramas de estados: Centrados en el estado cambiante de un sistema dirigido por eventos.
5. Diagramas de actividades: Centrados en el flujo de control de actividades.

***Diagramas de casos de uso*:** Representa un conjunto de casos de uso y actores (un tipo especial de clases) y sus relaciones. Los diagramas de casos de uso se utilizan para describir la vista de casos de uso estática de un sistema. Los diagramas de casos de uso son especialmente importantes para organizar y modelar el comportamiento de un sistema.
Es decir, un caso de uso es una descripción de las acciones de un sistema desde el punto de vista del usuario. Para los desarrolladores del sistema, ésta es una herramienta valiosa, ya que es una técnica de aciertos y errores para obtener los requerimientos del sistema desde el punto de vista del usuario.

Siguiendo el ejemplo que hemos venido analizando de las lavadoras, usted utiliza una lavadora, obviamente, para lavar ropa. La figura 2.9 Muestra como se representaría esto en un diagrama de casos de uso de UML. A la figura correspondiente al “usuario” se le conoce como actor. La elipse representa el caso de uso.

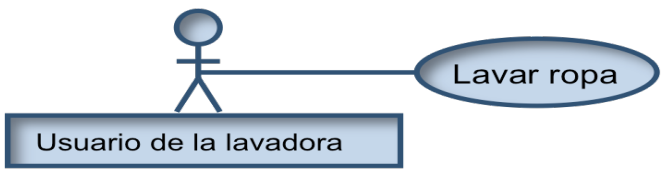

Figura 2.9 Diagrama de casos de uso UML

Diagramas de secuencia: Es un diagrama de interacción que resalta la ordenación temporal de los mensajes. Un diagrama de secuencia presenta un conjunto de objetos y los mensajes enviados y recibidos por ellos. Los objetos suelen ser instancias con nombre o anónimas de clases, pero también pueden representar instancias de otros elementos, tales como colaboraciones, componentes y nodos.

Los diagramas de secuencia se utilizan para describir la vista dinámica de un sistema.

El diagrama de secuencias UML muestra la mecánica de la interacción con base en tiempos.

Continuando con el ejemplo de la lavadora, entre los componentes de la lavadora se encuentran: una manguera de agua (para obtener agua fresca), un tambor (donde se coloca la ropa) y un sistema de drenaje.

¿Qué sucederá cuando llamemos al caso de uso lavar ropa? Si damos por hecho que completó las operaciones “agregar ropa”, “agregar detergente” y “activar”, la secuencia sería más o menos así:

- El agua empezará a llenar el tambor mediante una manguera.
- El tambor permanecerá inactivo durante 5 minutos.
- La manguera dejará de abastecer agua.
- El tambor girará de un lado a otro durante 15 minutos.
- El agua jabonosa saldrá por el drenaje.
- Comenzará nuevamente el abastecimiento de agua.
- El tambor continuará girando.
- El abastecimiento de agua se detendrá.
- El agua del enjuague saldrá por el drenaje.
- El tambor girará en una sola dirección y se incrementará su velocidad por 5 minutos.
- El tambor dejará de girar y el proceso de lavado habrá finalizado.

La figura 2.10 presenta un diagrama de secuencias que captura las interacciones que se realizan a través del tiempo entre el abastecimiento d agua, el tambor y el drenaje (representados como rectángulos en la parte superior del diagrama).

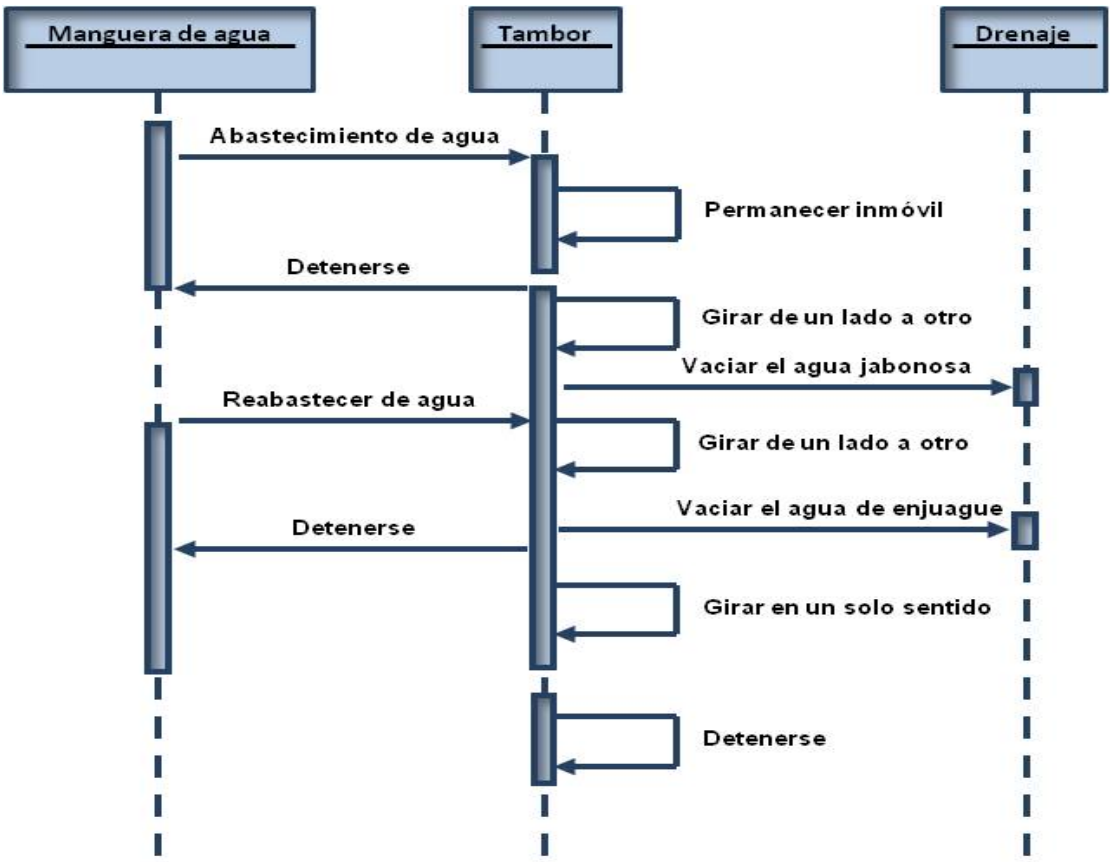

Figura 2.10 Diagramas de secuencia UML

Diagramas de colaboración: Es un diagrama de interacción que resalta la organización estructural de los objetos que envían y reciben mensajes. Un diagrama de colaboración muestra un conjunto de objetos, enlaces entre esos objetos y mensajes enviados y recibidos por esos objetos. Los objetos normalmente son instancias con nombre o anónimas de clases, pero también pueden representar instancias de otros elementos, como colaboraciones,

componentes y nodos. Los diagramas de colaboración se utilizan para describir la vista dinámica de un sistema. En la figura 2.11 Se muestra un cronometro interno al conjunto de clases que constituyen a una lavadora, luego de cierto tiempo, el cronómetro detendrá el flujo de agua y el tambor comenzará a girar de un lado a otro.

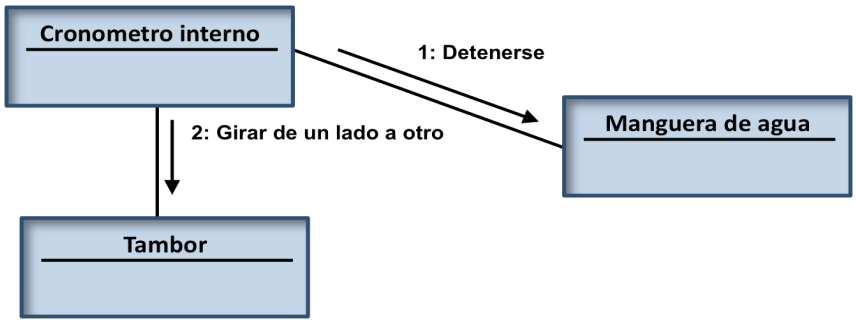

Figura 2.11 Diagrama de colaboraciones UML

***Diagramas de estados*:** Representa una máquina de estados, constituida por estados, transiciones, eventos y actividades. Los diagramas de estados se utilizan para describir la vista dinámica de un sistema. Son especialmente importantes para modelar el comportamiento de una interfaz, una clase o una colaboración. Los diagramas de estados resaltan el comportamiento dirigido por eventos de un objeto, lo que es especialmente útil al modelar sistemas reactivos.

La figura 2.12 muestra las transacciones de la lavadora de un estado al otro, el símbolo que está en la parte superior de la figura representa el estado inicial y el de la parte inferior es estafo final.

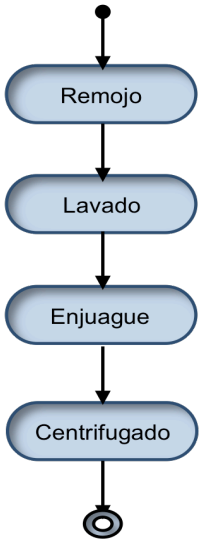

Figura 2.12 Diagrama de estados UML

Diagramas de actividades: Muestra el flujo de actividades de un sistema. Una actividad muestra un conjunto de actividades, el flujo secuencial o ramificado de actividades, y los objetos que actúan y sobre los que se actúa. Los diagramas de actividades se utilizan para ilustrar la vista dinámica de un sistema. Además, estos diagramas son especialmente importantes para modelar la función de un sistema, así como para resaltar el flujo de control entre objetos.

Las actividades que ocurren dentro de un caso de uso o dentro del comportamiento de un objeto se dan, normalmente, en secuencia, como en los pasos que están de ejemplo en los diagramas de secuencia.

La figura 2.13 muestra la forma en que el diagrama de actividades UML representa alguno de los pasos mencionados en el diagrama de secuencias.

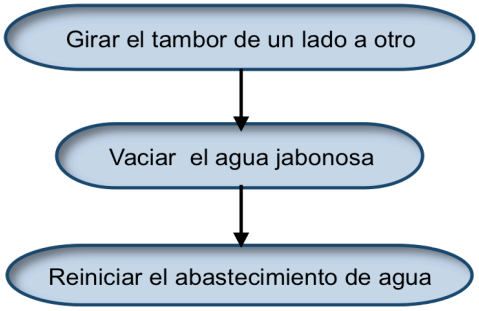

Figura 2.13 Diagramas de actividades UML

2.2.4 Ventajas de UML contra otros lenguajes

Algunas ventajas que encontramos en UML son:

- Su unificación, esto quiere decir que nos permite que sea interpretado por cualquier analista en cualquier parte del mundo.
- Es una notación estándar para el modelado de sistemas Software UML no es un proceso de desarrollo es decir, no describe los pasos sistemáticos a seguir para desarrollar software.

- Modela sistemas mediante el uso de objetos que forman parte de él así como, las relaciones estáticas o dinámicas que existen entre ellos.
- Es totalmente orientada a objetos.
- Facilita la realización del diseño en menos tiempo.
- Disminuye la complejidad para la realización de algún software.

2.2.5 Justificación del uso de UML

Se decidió el uso de este lenguaje ya que es el utilizado para la documentación de la metodología de RUP.

Por otra parte RUP propone usar UML para llevar la documentación del sistema, facilitar la etapa del diseño para su posterior construcción o desarrollo, así como transmitir ideas y ayudar al equipo a comunicarlas.

No hay que olvidar que UML y RUP son dos cosas distintas. Mientras que UML es sólo un lenguaje visual y de modelado, RUP es un modelo o proceso de desarrollo de software, es por ello que se complementan para el mejor desarrollo y entendimiento del diseño del sistema.

Para efectos de seguridad del proyecto se necesita la implementación de mecanismos criptográficos los cuales se describen a continuación.

2.3 Mecanismos criptográficos para la autenticidad y confidencialidad.

La criptografía es el estudio de técnicas matemáticas relacionadas a los aspectos de seguridad de la información como la confidencialidad, integridad de los datos, autenticación de la entidad, y autenticación de origen de los datos.

Para el cumplimiento de las metas criptográficas existen las primitivas criptográficas, que haciendo usos de esquemas de cifrado, funciones hash y esquemas de firma digital cumplen con las mismas.

2.3.1 Primitivas criptografías

Son la función más básica que compone un sistema criptográfico, existen la primitiva de cifrado, la primitiva de descifrado, la primitiva de firma, la primitiva de verificación de firma etc.

Ayudan a cumplir con las características de la información, haciendo uso de:

- Esquemas de Cifrado.
- Funciones hash.
- Esquemas de firma digital.

Adicionalmente los criterios que deben evaluarse son:

- Nivel de seguridad. Esto es difícil de cuantificar sin embargo, típicamente el nivel de seguridad se define por un límite superior en la cantidad de trabajo necesario para frustrar el objetivo.
- Funcionalidad: las propiedades de las primitivas determinan la necesidad de combinarse para garantizar varias características de la seguridad de la información.
- Métodos de operación cuando se aplican varias maneras y con varias entradas se exhibirán típicamente diferentes características. Así, una primitiva podría proporcionar diferente funcionalidad, la cual depende de la forma de funcionamiento o uso.
- Función: se refiere a la eficacia de la primitiva en un modo de funcionamiento en particular.
- Facilidad de implementación. Involucra la complejidad de llevar a cabo la primitiva en software o en ambiente hardware.

2.3.2 Cifrado

El cifrado es un método que permite implementar el servicio de seguridad de un mensaje o de un archivo mediante la codificación del contenido, por medio de operaciones matemáticas, de manera que sólo pueda leerlo la persona que cuente con dicha clave de cifrado para decodificarlo.

Los procesos de cifrado y descifrado son las operaciones fundamentales en la criptografía, las cuales integran operaciones conocidas como algoritmos

criptográficos y que en conjunto con un elemento único de transformación, conocido como llave, actúa sobre el texto claro para obtener el texto cifrado.

Todos estos elementos conforman un criptosistema. Es decir, los criptosistemas se basan en la dificultad de deshacer esas operaciones como base para una comunicación segura.

Los actuales esquemas de cifrado se dividen en 2 grupos, los esquemas simétricos y los esquemas asimétricos.

- Esquema Simétrico: es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. En la figura 2.14 se ilustra como las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.

Es decir, si una entidad ajena se apodera de la llave secreta, el criptosistema se compromete y la llave debe ser desechada.

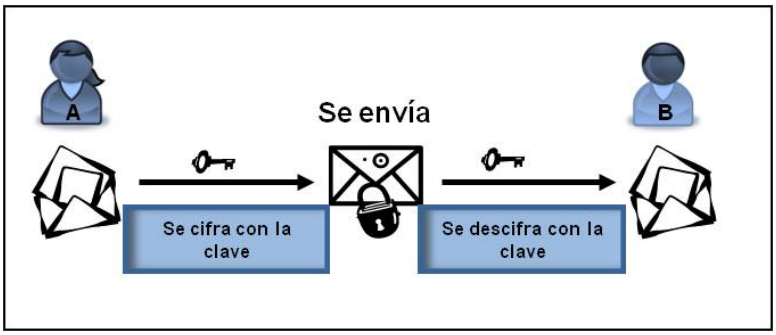

Figura 2.14 Cifrado Simétrico

Los esquemas simétricos se pueden clasificar en dos grupos, los cifrados de bloques y los cifrados de flujo.

Cifrado de bloque: Este tipo de cifrado se opera sobre el texto claro formando grupos de bits de longitud fija llamados bloques de entrada, convirtiendo cada uno de ellos en un bloque cifrado. Este procedimiento se repite hasta cifrar todos los bloques que en conjunto forman el texto cifrado.

Cifrado de flujo: Este tipo de cifrado se efectúa en tiempo real mediante la función XOR entre pequeñas muestras del texto claro de uno o varios bits y la llave obtenida por un generador de flujo de llaves. Las salidas se conectan para obtener el texto cifrado.

- Asimétrico: es un método criptográfico que usa un par de claves para el cifrado de mensajes. Las dos claves, representadas en la figura 2.15 con dos llaves diferentes, pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier entidad, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella.

  Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

  De esta manera si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado este, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad en el envío del mensaje. El orden de uso de cada llave varía de acuerdo al objetivo de la aplicación, cuando en el emisor se conforman los servicios de autenticación y no repudio, como el caso de la firma digital.

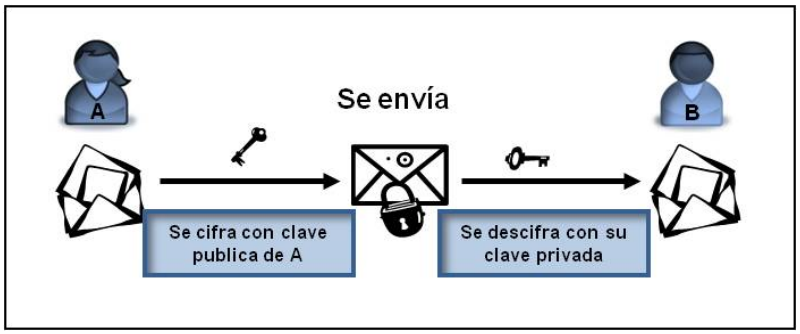

Figura 2.15 Cifrado Asimétrico

Por otro lado si el emisor cifra con la llave pública del receptor, este último debe descifrar con su llave privada asegurando así entre emisor y receptor el servicio de confidencialidad.

2.3.3 Funciones hash

La principal tarea de las funciones hash es comprimir la información en bloques de longitud fija. Estas funciones son públicas y tienen la característica de ser diferentes de las funciones clásicas de compresión.

Las funciones hash no son reversibles, es decir a partir del bloque de longitud fija, no se puede recuperar el mensaje original. Sin embargo deben de cumplir con las siguientes condiciones.

- Transformar un texto de longitud variable en un bloque de longitud fija.
- Ser irreversibles
- Conocido un lenguaje y su función hash debe ser imposible encontrar otro mensaje con la misma función.
- Es imposible inventar dos mensajes cuya función hash sea la misma.

2.3.4 Firma digital

La firma digital es un control criptográfico primitivo, fundamentalmente utilizada para garantizar autenticación, autorización y no repudio ante una tercera entidad.

Su propósito es ligar la información a la identidad de una entidad, debido a que funciona como un sello digital que se añade a los datos que se envían y sirve para comprobar si alguien ha modificado el contenido de la información, además de garantizar que una entidad envió dichos datos. Consiste en dos procesos fundamentales: firma de los datos y validación de la firma.

El proceso de firma de datos: este no cifra todo el mensaje, se hace sobre un resumen de la información (hash), el resumen se transforma por medio de la llave privada, los datos cifrados resultantes se añaden al mensaje original, se envía al destinatario el paquete compuesto por el mensaje original, y la firma. Mientras tanto, por medio de la llave pública se elimina la transformación hecha sobre el hash de mensaje. En la figura 2.16 se puede observar que se comparan los dos resúmenes obtenidos y si son iguales el mensaje es autentico y la verificación es verdadera. En caso contrario la firma es falsa.

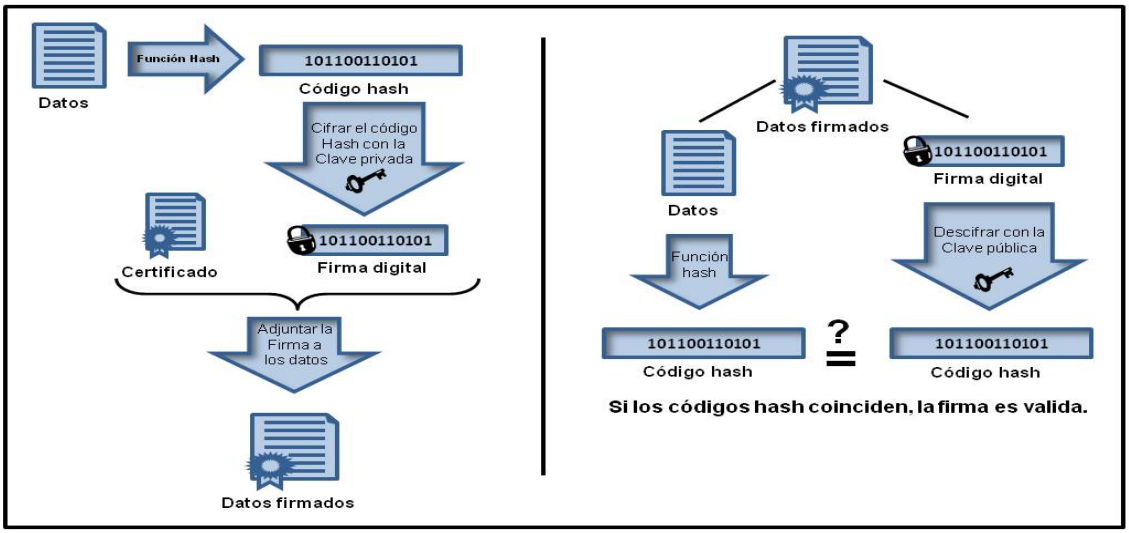

Figura 2.16 Funciones Hash y Firma Digital

CAPÍTULO III

WORKFLOW DE LOS REQUISITOS

3.1 Workflow de los Requisitos

En este capítulo se lleva a cabo la identificación de los requisitos necesarios para el diseño del sistema, así como el análisis del problema mediante la metodología RUP como se muestra en la figura 3.1, basada en el modelo de representación de dicha metodología, el cual muestra el desarrollo del flujo de trabajo (workflow), así como las actividades realizadas dentro del mismo.

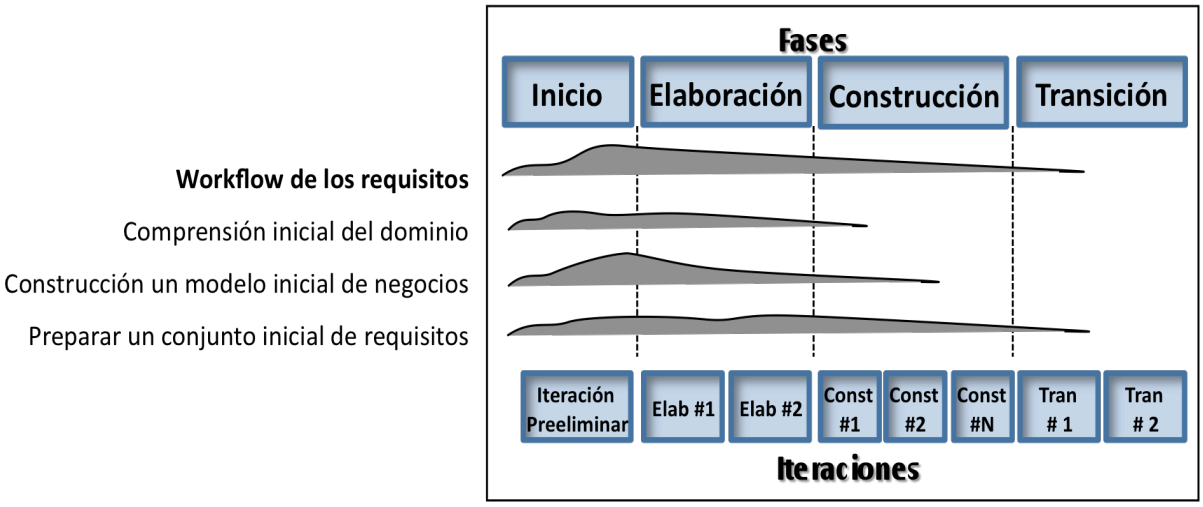

Figura 3.1 Diagrama de Fases del Workflow de los requisitos

Como ya se había mencionado en el capitulo anterior, el objetivo de este paso es asegurar que los desarrolladores construyan el sistema de información correcto, esto se logra describiendo el sistema de información objetivo de forma clara, detallada y precisa, de tal manera que sean comprendidos completamente por el cliente.
Para ello se trabajo con el siguiente diagrama, figura 3.2.

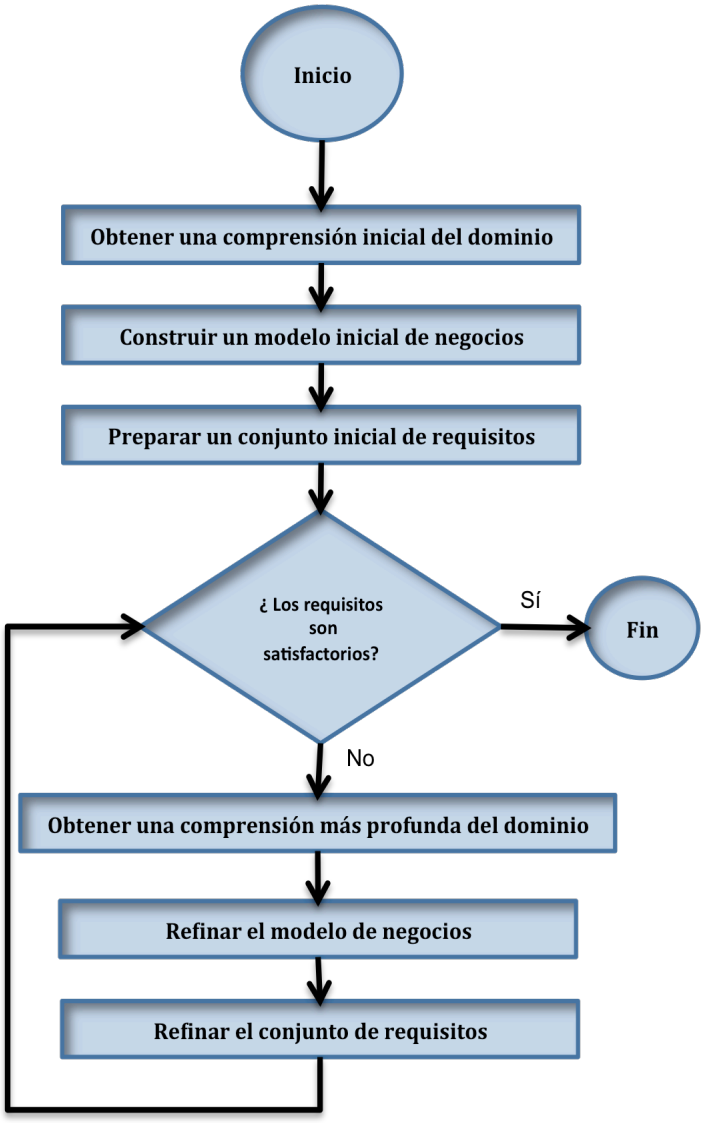

Figura 3.2 Diagrama del Workflow de los Requisitos.

3.1.1 Obtener una comprensión inicial del dominio

Para el desarrollo de esta primera tarea se utilizó como herramienta los cuestionarios (véase anexo I).

Estos fueron elaborados con el propósito de tener un panorama del manejo del memorándum en áreas estratégicas de la Institución, obteniendo como resultado la descripción del proceso. Este se centra en envió, recepción y almacenaje de dichos documentos, los cuales se describen a continuación:

Proceso de generación:

1.- El remitente genera un archivo en cualquier procesador de textos, de manera general agrega los siguientes datos:

- No. Folio (generado a través de una bitácora manual) número de consecutivo, con las siglas del departamento y el año. (el número de consecutivo deberá contener las primeras siglas del nombre del departamento, más el número consecutivo del memorándum, más los dos últimos dígitos del año correspondiente, separados por una diagonal).
- Leyenda memorándum
- Fecha
- Servidor a quien va dirigido presidido por la expresión “Para”
- Puesto del servidor a quien va dirigido
- Nombre del que suscribe el memorándum precedido por la expresión “De”
- Puesto de quien emite el memorándum
- Redacción en forma breve
- Al termino del memorándum se anota la expresión “Atentamente”
- Las abreviaturas c.c.p.

2.- Imprime la cantidad de hojas necesarias para hacer llegar las copias a los destinatarios y su respectivo acuse de recibo.

3.- Firma, con firma autógrafa el memorándum original, y las copias con facsímil.

Proceso de envió:

1.- Una persona comisionado (mensajero) se encarga de la entrega de dicho documento, éste debe trasladarse hasta la oficina de cada destinatario.
2.- Realiza la entrega a quién indique serlo o bien a quién mencione tener la facultad para recibirlo (solo el personal adscrito al área correspondiente).
3.- Solicita la firma (sello) en el acuse de recibo y entrega una copia del documento.
4.- Regresa a la oficina a entregar el acuse de recibo firmado por destinatarios

Proceso de Recepción:

1.- El destinatario verifica que su nombre este anexo al memorándum.
2.- Firma el acuse de recibo y recibe la copia.

Proceso de Almacenaje:

1.- El remitente del memorándum tiene la obligación de archivar una copia de dicho documento así como su acuse de recibo, en orden consecutivo de folio.

Proceso de Búsqueda:

1.- Se realiza la búsqueda en el archivero por folio de memorándum (solo el funcionario responsable del área).
2.- Se le proporciona una copia al usuario.
3.- Se regresa al archivero de acuerdo a folio.

3.1.2 Construir un modelo inicial de negocios

Con el análisis de las herramientas utilizadas se obtuvieron, una serie de requerimientos, Tabla 1:

Requerimientos funcionales	Requerimientos no funcionales
• Generación de número consecutivo – Folio • Plantilla con componentes básicos. • Seguridad (Autenticación) en los procesos de: generación, envió, recepción, almacenaje y búsqueda • Rapidez en los procesos de: generación, envió, recepción, almacenaje y búsqueda. • Uso de contraseña.	• PC Hw: Intel Core Dos 3.0 GHz, 2GB en Ram, 250 GB • Plataforma: Windows, Windows XP, Windows Vista, Windows 7 • Paquetería Office 2007, Visual Studio • Conexión a internet: STM1 • Servidor de aplicaciones: SAES • No se cuenta con Intranet

Tabla 1 Requisitos Funcionales

3.1.3 Preparar un conjunto inicial de requisitos

En esta actividad del análisis de requisitos, solo se tomaron los requerimientos funcionales, ya que estos especifican una acción que el sistema de información debe ser capaz de realizar [5].

De estos requisitos, se obtuvieron los casos de uso, los cules se describen en un formato que detalla su proceso.

El caso de uso general figura 3.3, comprende la construcción inicial de negocios.

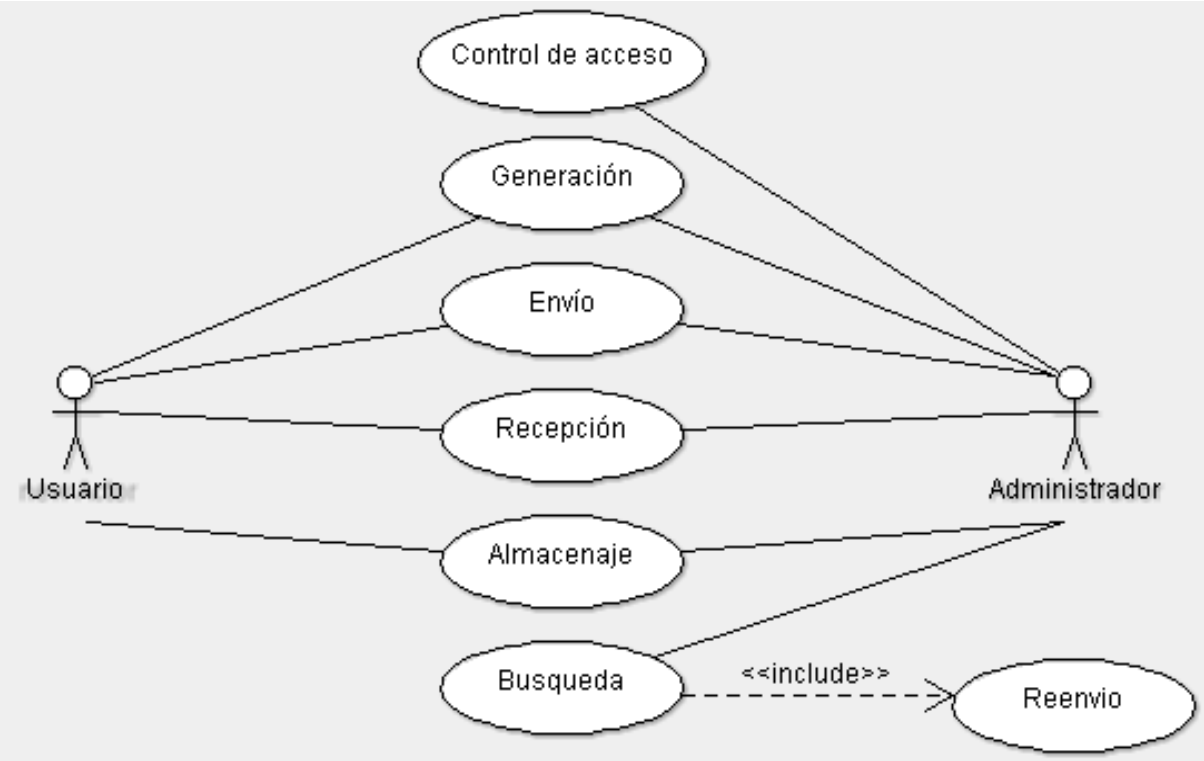

Figura 3.3 Diagrama Casos de uso Sistema de Gestión de Memorándums

A continuación se muestra cada diagrama de caso de uso con un formato, el cual como ya se había mencionado describe y detalla dicho diagrama.

El caso de uso “control de acceso” figura3.4, muestra como se va a llevar a cabo el acceso al sistema, así como también las acciones que podrá desarrollar cada operador dentro del mismo.

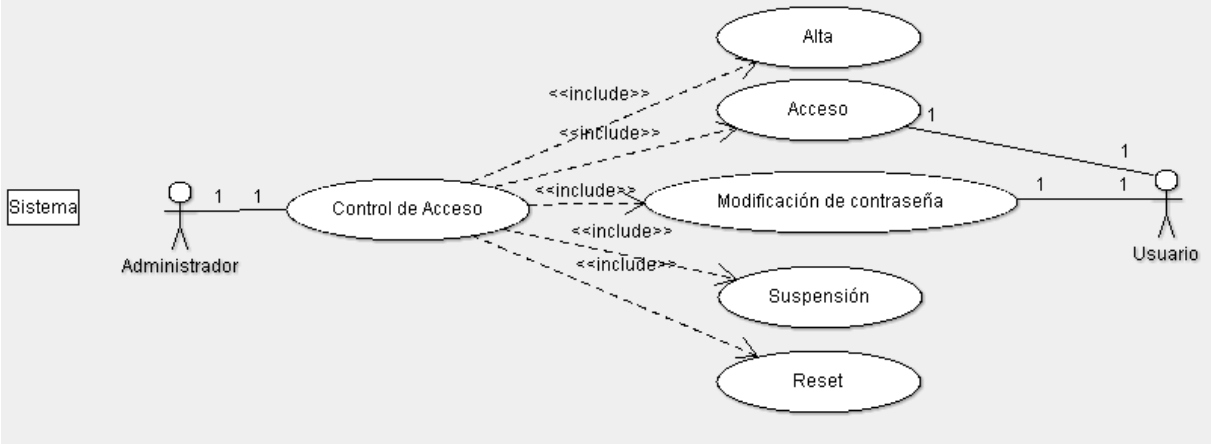

Figura 3.4 Diagrama Caso de uso Control de Acceso

Caso de Uso	CONTROL DE ACCESO	
Acción	I. Acción “alta en el sistema”	
Descripción	El caso de uso *control de acceso* permitirá la administración del sistema así como el ingreso al mismo por parte de los usuarios. El sistema requerirá al administrador los siguientes datos para dar de alta a los nuevos usuarios: 1. Nombre completo del usuario (apellido paterno, materno y nombres). 2. Departamento o área a la que corresponde. 3. Cargo con el que cuenta el usuario en el departamento. 4. El id de usuario debe estar compuesto por las tres primeras letras del nombre, más las tres primeras letras del apellido paterno y más el número consecutivo que asigne el sistema.	
Precondición	El administrador deberá de estar dado de alta en el sistema. El solicitante deberá contar con una cuenta de usuario válida ó autorizada para iniciar sesión dentro de la ESIME Culhuacan. Contar con un equipo de cómputo conectado a una red con acceso autorizado al servidor de la aplicación. La contraseña deberá ser de 8 caracteres y de tipo alfanumérica. La palabra clave deberá ser de 6 caracteres.	
Secuencia normal	**Paso**	**Acción**
	1	El administrador ingresa los datos del usuario a dar de alta.
	2	Si el usuario ya estaba dado de alta. Excepción DUPLICIDAD
	3	Cuando el usuario ingresa por primera vez al sistema, su contraseña va a hacer igual a su “id de usuario”
	4	Una vez el usuario teniendo acceso al sistema como se planteo en el punto anterior, se le pide cambiar su contraseña e ingresar una palabra clave.
	5	Si los datos ingresados por parte del usuario no son correctos, excepción ALTA
Postcondición	Una vez dado de alta, el usuario es el único responsable del buen uso de su ID y contraseña.	
Excepciones	**Excepción DUPLICIDAD**	
	1 El sistema mandará un mensaje de error al identificar registros duplicados.	
	Excepción ALTA	
	Paso	**Acción**
	1	Despliega un mensaje de error
	2	El usuario puede nuevamente ingresar su id de usuario y contraseña
Frecuencia esperada	Cada vez que se tenga que dar de alta a un usuario en el sistema	
Importancia	Indispensable para controlar el acceso al sistema	

Caso de Uso	CONTROL DE ACCESO
Acción	II. Acción “acceso al sistema login”
Descripción	El administrador y usuario podrán tener acceso al sistema, de acuerdo a su perfil de usuario.
Precondición	El usuario deberá de estar dado de alta en el sistema El id de usuario deberá estar compuesto por las tres primeras letras del nombre, más las tres primeras letras del apellido paterno y más el

	número consecutivo que asigne el sistema. La contraseña deberá de ser de 8 caracteres y de tipo alfanumérica.	
Secuencia normal	**Paso**	**Acción**
	1	El administrador puede ingresar al sistema de acuerdo setup.
	2	El usuario para tener acceso al sistema debe de ingresar su "id de usuario" y contraseña, dando la instrucción de acceso al sistema
	2ª	Si el id de usuario y contraseña son correctos podrá tener acceso exitosamente
	2B	Si el id de usuario y/o contraseña son incorrectos se procede a la excepción ACCESO.
Postcondición	Por seguridad el sistema ejecutará cada mes la acción modificación de contraseña.	
Excepciones	**Excepción ACCESO**	
	Paso	**Acción**
	1	Si id de usuario y/o contraseña son erróneos mostrará un mensaje de error.
	2	Contará con tres intentos para ingresar los datos correctos.
	3	Si en los tres intentos los datos ingresados por el usuario son incorrectos se procederá al bloqueo de los mismos.
Frecuencia esperada	Una vez por cada usuario por cada intento de acceder al sistema	
Importancia	Indispensable para controlar el acceso al sistema	

Caso de Uso	CONTROL DE ACCESO	
Acción	III. Acción "desbloqueo de contraseña"	
Descripción	Esta acción permitirá al usuario desbloquear su contraseña, si es que éste no pudiera desbloquearla acudiría al administrador para que le haga el desbloqueo de la misma.	
Precondición	El usuario deberá de estar dado de alta en el sistema. El usuario deberá estar logado en el sistema. La contraseña deberá haber sido bloqueada. El usuario deberá recordar su palabra clave para el desbloqueo de contraseña. Identificar que el usuario a desbloquear sea quien dice ser, mostrando una identificación oficial para la ESIME Culhuacan con fotografía. Validar que el usuario a desbloquear aun siga facultado para tener acceso al sistema.	
Secuencia normal	**Paso**	**Acción**
	1	El usuario solicita al sistema el desbloqueo de contraseña.
	2	El sistema pide al usuario su id de usuario y la palabra clave.
	2ª	Si la palabra clave introducida es errónea. Excepción CLAVE
	3	Si el usuario no recuerda su palabra clave, el desbloqueo lo realizará el administrador.
	4	El administrador procederá a realizar los pasos de la acción "reset paso ¿?"
Postcondición	Ninguna	
Excepciones	**Excepción CLAVE**	
	Paso	**Acción**

	1	El sistema mostrará un mensaje de error.
	2	El usuario contará con tres intentos para ingresar la palabra clave.
	3	Si en los tres intentos la clave es incorrecta se deshabilita la opción de desbloqueo.
Frecuencia esperada	Una vez que el usuario lo solicite por cada vez que su contraseña sea bloqueada	
Importancia	Indispensable para que el usuario pueda tener acceso al sistema	
Urgencia	Inmediata cuando el administrador ejecute el procedimiento de alta en el sistema paso 1.	

Caso de Uso	CONTROL DE ACCESO	
Acción	IV. Acción “modificación de contraseña”	
Descripción	Esta acción permitirá al usuario modificar su contraseña si así lo desea en el momento que lo requiera ó si el sistema lo solicita.	
Precondición	El usuario deberá estar dado de alta en el sistema. El usuario deberá estar logado en el sistema. El usuario deberá tener la necesidad de hacer un cambio de contraseña. Que la contraseña haya expirado. La contraseña nueva contraseña debe ser diferente a la actual y contar con las características establecidas en la acción alta al sistema.	
Secuencia normal	**Paso**	**Acción**
	1	El usuario ó sistema solicita la modificación de contraseña.
	2	El usuario ingresará su id de usuario y la contraseña con la que cuenta actualmente
	3	El sistema pide al usuario ingresar la nueva contraseña
	4	El sistema para validarla pide que la ingrese nuevamente y es así como se lleva la actualización de la contraseña
	5	Si la contraseña ingresada por el usuario no es válida, según las características de la misma, excepción ALTA
Postcondición	Una vez efectuada la modificación de la contraseña, el usuario es el único responsable del buen uso de su ID y contraseña.	
Excepciones	**Excepción ALTA**	
	Paso	**Acción**
	1	Si id de usuario y/o contraseña son erróneos mostrara un mensaje de error
	2	Contara con tres intentos para ingresar los datos correctos
	3	Si en los tres intentos los datos ingresados por el usuario son incorrectos se procederá al bloqueo de los mismos
Frecuencia esperada	Una vez que el usuario lo solicite por cada modificación de contraseña	
Importancia	Indispensable para que el usuario pueda tener acceso al sistema	
Urgencia	Inmediata cuando el usuario ejecute el procedimiento de modificar contraseña	

Caso de Uso	CONTROL DE ACCESO	
Acción	V. Acción de “suspensión”	
Descripción	Permitirá al administrador suspender a los usuarios que ya no deben tener acceso al sistema	
Precondición	El usuario deberá de estar dado de alta en el sistema. El administrador deberá estar logado en el sistema. Contar con una solicitud de suspensión de usuario. Validar que el usuario ya no este facultado para tener acceso al sistema.	
Secuencia normal	**Paso**	**Acción**
	2	El administrador ingresa el id del usuario a suspender.
	1	El administrador solicita la suspensión.
	3	El sistema muestra los datos de las coincidencias pide la confirmación al administrador si realmente está seguro de querer suspender el acceso al usuario seleccionado. Excepción id inexistente
	4	El administrador valida los datos con la solicitud
	5	El administrador solicita mediante la acción directa de suspensión
	6	El sistema pide la confirmación al administrador si realmente está seguro de querer suspender el acceso al usuario.
	6A	Si la confirmación del usuario a suspender es positiva ejecutar la acción de suspensión
	6B	Si la confirmación del usuario a suspender es negativa se cancela la acción.
Postcondición	Dar conocimiento al área correspondiente de que el usuario ya fue suspendido.	
Excepciones	**Excepción id inexistente**	
	Paso	**Acción**
	1	El usuario a suspender no existe en el sistema
	2	El usuario a suspender ya fue suspendido del sistema.
Frecuencia esperada	Una vez por cada solicitud de suspensión	
Importancia	Indispensable para garantizar el no acceso a usuarios no facultados	
Urgencia	Inmediata cuando se tenga una solicitud generada	

Caso de Uso	CONTROL DE ACCESO	
Acción	VI. Acción “reset”	
Descripción	El administrador podrá dejar en blanco la contraseña de los usuarios.	
Precondición	El usuario deberá de estar dado de alta en el sistema. El administrador deberá estar logado en el sistema. Que el usuario haya deshabilitado la opción de desbloqueo. Que la solicitud sea realizada por parte del usuario a restablecer.	
Secuencia normal	**Paso**	**Acción**
	1	El administrador ingresa el id del usuario a restablecer.
	2	El administrador solicita el reset del usuario mediante una acción directa
	3	El sistema blanquea la contraseña del usuario y se ejecuta la acción alta en el sistema paso 4.
Postcondición	Una vez concluida exitosamente la acción reset el usuario puede	

	tener acceso al sistema como se planteo en la acción acceso al sistema
Frecuencia esperada	Cada vez que exista una solicitud
Importancia	Indispensable para que el usuario pueda hacer uso del sistema
Urgencia	Inmediata

El caso de uso “generación” figura 3.5, detalla cómo se va a llevar a cabo la creación del memorándum, cómo va hacer el proceso de firma, así como también la manera en que se va a llevar a cabo el almacenamiento del mismo.

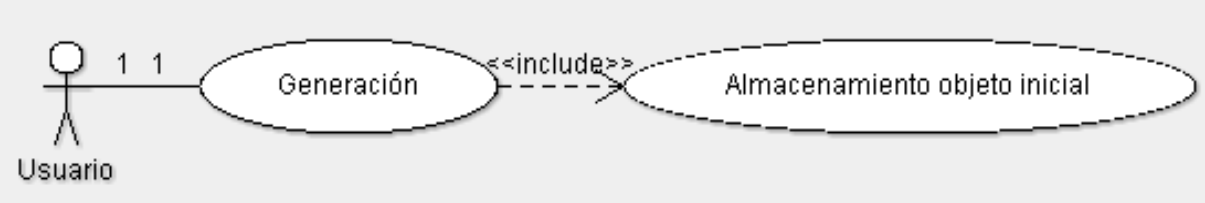

Figura 3.5 Diagrama Caso de Uso Generación

Caso de Uso	GENERACIÓN	
Acción	Acción “generación”	
Descripción	El caso de uso *generación* permite la creación del memorándum Esta acción permitirá al usuario llenar el memorándum establecido en la plantilla	
Precondición	El usuario deberá estar dado de alta en el sistema. El usuario deberá estar logado en el sistema. Los requisitos básicos que deberá contener la plantilla para el memorándum son: • leyenda memorándum • formato fecha • servidor a quien va dirigido, precedido por la expresión “Para:” • puesto del servidor a quien va dirigido • nombre del que suscribe el memorándum, precedido por la expresión “De:” • puesto de quien emite el memorándum • redacción en forma breve • al término del memorándum se anota la expresión “Atentamente:” • las abreviaturas c.c.p. (con copia para) • número de consecutivo, con las siglas del departamento y el año. (el número de consecutivo deberá contener las primeras siglas del nombre del departamento, más el número consecutivo del memorándum, más los dos últimos dígitos del año correspondiente, separados por una diagonal)	
Secuencia normal	**Paso**	**Acción**
	1	El usuario llena la plantilla del memorándum a generar.
	2	El usuario guarda dicha información en el sistema, de manera temporal

	3	El usuario puede suspender el envió del memorándum y guardarlo para su posterior envió. En este caso el memorándum queda en estado de borrador.
	4	El usuario solicita la acción de firmar, el sistema despachará una aplicación que realice el proceso de firmado. Esta aplicación estará inicializada con la información del memo a generar que incluya el contenido del mismo remitente y destinatario.
	5	Una vez que la aplicación se ejecuta en el ambiente local, esta solicitará la llave privada del usuario y procederá a generar la firma digital inmediatamente, eliminando de manera segura la copia de la llave privada del usuario.
	6	Una vez que el memorándum se encuentra firmado, este será enviado de regreso al sistema para su almacenamiento y referencia al destinatario como mensaje nuevo.
	7	Una vez que la aplicación local obtenga el acuse de recibo de parte del sistema, la aplicación deberá blanquear datos sensibles (borrado seguro) y procederá a destruirse.
Postcondición	El usuario es responsable del contenido del memorándum que generó.	
Frecuencia esperada	Cada vez que el usuario requiera llevar a cabo la generación de un memorándum.	
Importancia	Indispensable para la comunicación entre los usuarios en cuanto a los memorándums generados.	

El caso de uso “envío” figura 3.6, muestra cómo se va a llevar a cabo el envío del memorándum, así como los operadores que podrán hacer dicha acción.

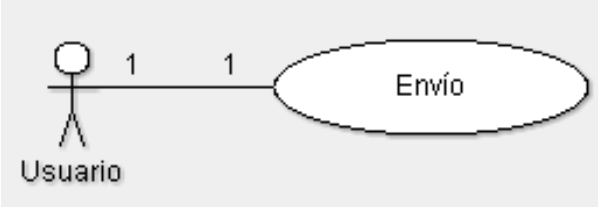

Figura 3.6 Diagrama Caso de Uso Envió

Caso de Uso	ENVIO	
Acción	I. Acción “envío”	
Descripción	Esta acción permitirá el envío del memorándum	
Precondición	El usuario deberá estar dado de alta en el sistema. El usuario deberá estar logado en el sistema. El usuario deberá contar con un memorándum ya generado.	
Secuencia normal	**Paso**	**Acción**
	1	El usuario ingresa los datos del destinatario a quien va dirigido el memorándum.

	2	El sistema pregunta al usuario si los destinatarios son los correctos. Excepción ENVIO
	3	El usuario solicita mediante la acción directa enviar
Postcondición	Es responsabilidad del usuario que envía el memorándum del contenido del mismo.	
Excepciones	**Excepción envío**	
	Paso	**Acción**
	1	El usuario puede corregir al destinatario.
Frecuencia esperada	Cada vez que el usuario requiera llevar a cabo el envío de un memorándum	
Importancia	Indispensable para la comunicación entre los usuarios	

El caso de uso “recepción”, muestra cómo se va a llevar a cabo la recepción del memorándum, así como los operadores que podrán hacer dicha acción.

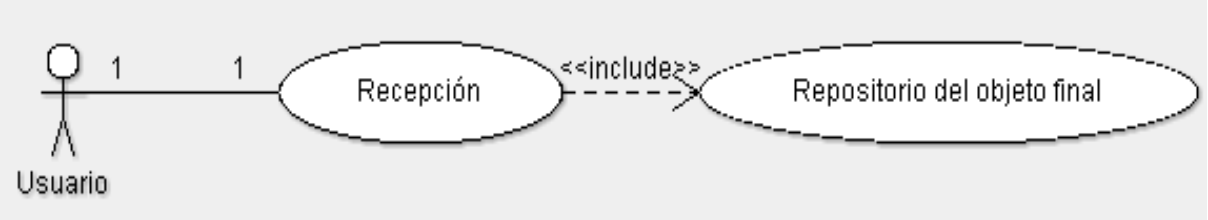

Figura 3.7 Diagrama Caso de Uso Recepción

Caso de Uso	RECEPCIÓN	
Acción	I. Acción “recepción”	
Descripción	Esta acción permitirá al usuario recibir el memorándum que le ha sido enviado.	
Precondición	El usuario deberá estar dado de alta en el sistema. El usuario deberá estar logado en el sistema. La recepción identifica al remitente y el título del memorándum para proceder a su recepción o incorporase a una lista de pendientes.	
Secuencia normal	**Paso**	**Acción**
	1	Al usuario le llegará un mensaje de que tiene un memorándum pendiente de leer.
	2	Si el usuario desea en ese momento leer el memorándum solicitará la acción directa de leer
	3	Si el usuario no desea leer el memorándum en ese momento, este quedará en un status pendiente de leer.
	4	Cuando el usuario desee leer el memorándum se procede la acción recepción punto 2
Postcondición	El memorándum se almacena en un repositorio del objeto final. Si el memorándum es privado el usuario receptor deberá contar con su llave privada para poder leer el memorándum	
Frecuencia esperada	Cada vez que el usuario reciba un memorándum	
Importancia	Indispensable para la comunicación entre los usuarios	

El caso de uso “búsqueda” figura 3.8, detalla como se va a realizar la búsqueda de un memorándum, así como también las acciones que a partir de esta resulten.

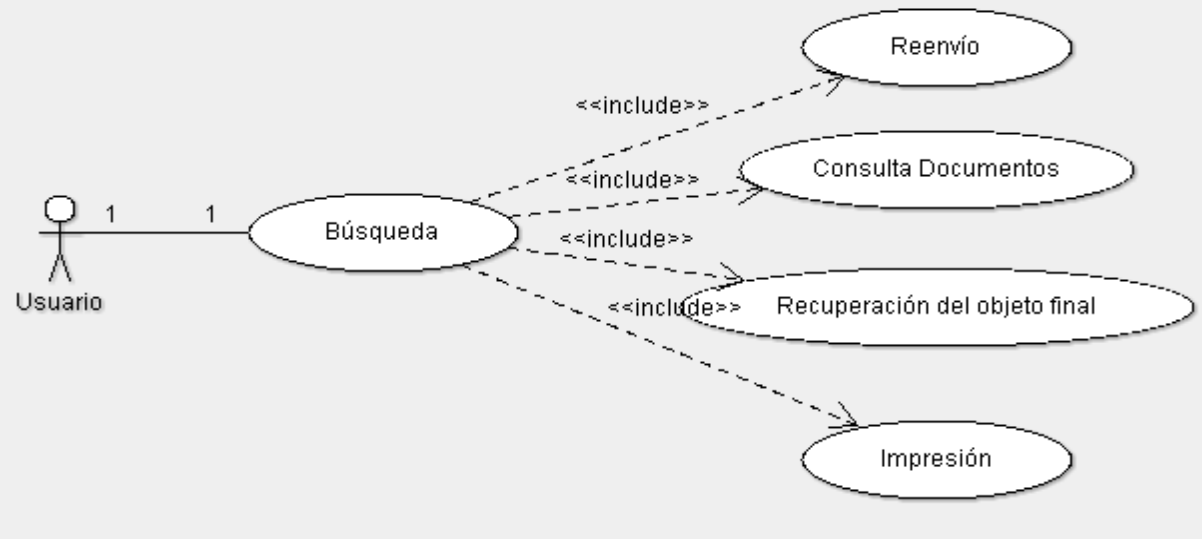

Figura 3.8 Diagrama Caso de Uso Búsqueda

Caso de Uso	BÚSQUEDA	
Acción	I. Acción “búsqueda”	
Descripción	La *búsqueda* permitirá al usuario el reenvío, consulta, recuperación e impresión del memorándum deseado. Esta acción permite al usuario realizar una búsqueda específica o no de un memorándum.	
Precondición	Que el memorándum a buscar tenga el tiempo de vigencia establecido por cada área para ser guardado en sistema	
Secuencia normal	Paso	Acción
	1	El usuario puede realizar la búsqueda de algún memorándum en específico por el número de folio.
	2	El usuario puede realizar la búsqueda de algún memorándum no específico haciendo una consulta ya sea por: • Día/Mes/Año en que se elaboró el memorándum o en que fue recibido • Mes/Año en que se elaboró el memorándum o en que fue recibido • Año en que se elaboró el memorándum o en que fue recibido • Persona a quien fue dirigido • Persona quien fue el remitente • Por palabras clave que contenga el memorándum.
	3	El usuario selecciona la opción de buscar.
	4	El sistema muestra una pantalla donde puede ingresar la información a buscar ya sea específica o no específica.

Postcondición	Si no existen los datos a buscar, o existen más de 2 documentos con el mismo nombre, pueden ocurrir las siguientes acciones	
Excepciones	Excepción BUSQUEDA	
	Paso	Acción
	1	No existe el memorándum con ese nombre.
	2	Si existe más de 1 memorándum con ese nombre, el sistema mostrara una lista de los memorándums encontrados y los mostrara.
Frecuencia esperada	Las veces que sean necesarias	
Importancia	Indispensable para la localización y/o ubicación de un memorándum	
Urgencia	Inmediata cuando no se tiene una sesión establecida previamente o en el caso de que ésta haya caducado.	
Comentarios	Se debe diseñar una base de datos o repositorio	

Caso de Uso	BÚSQUEDA	
Acción	I. Acción “REENVIO”	
Descripción	Esta acción permitirá el reenvío del memorándum que se recibió o se busco y se encontró con éxito.	
Precondición	El usuario deberá estar dado de alta en el sistema. El usuario deberá estar logado en el sistema. El usuario deberá contar con un memorándum seleccionado para poderlo reenviar.	
Secuencia normal	**Paso**	**Acción**
	1	El usuario ingresa al sistema seleccionando la opción de búsqueda mediante los pasos de la acción 1 “búsqueda”.
	2	El sistema pregunta al usuario si los destinatarios son los correctos. Excepción ENVIO
	3	El usuario solicita mediante la acción directa reenviar
Postcondición	Es responsabilidad del usuario que reenvía el memorándum del contenido del mismo.	
Excepciones	**Excepción envío**	
	Paso	**Acción**
	1	El usuario puede corregir al destinatario.
Frecuencia esperada	Cada vez que el usuario requiera llevar a cabo el reenvió de un memorándum	
Importancia	Indispensable para la comunicación entre los usuarios	

Caso de Uso	BÚSQUEDA	
Acción	I. Acción “CONSULTA”	
Descripción	Esta acción permitirá la consulta del memorándum	
Precondición	El usuario deberá estar dado de alta en el sistema. El usuario deberá estar logado en el sistema.	
Secuencia normal	**Paso**	**Acción**
	1	El usuario ingresa al sistema seleccionando la opción de consulta memorándum.
	2	El sistema pregunta al usuario los datos para generar la consulta del memorándum.
	3	El usuario solicita mediante la acción directa consultar, si los datos son incorrectos o no existen. Excepción CONSULTA
Excepciones	**Excepción envío**	
	Paso	**Acción**

	1	El usuario puede corregir al destinatario.
Frecuencia esperada	Cada vez que sea necesario realizar una consulta	

Caso de Uso	BÚSQUEDA	
Acción	I. Acción “RECUPERACION”	
Descripción	Esta acción permitirá la recuperación del memorándum recibido o almacenado en el sistema	
Precondición	El usuario deberá estar dado de alta en el sistema. El usuario deberá estar logado en el sistema.	
Secuencia normal	**Paso**	**Acción**
	1	El usuario ingresa los datos a recuperar del memorándum ya buscado.
	2	El usuario solicita mediante la acción directa de recuperación.
Frecuencia esperada	Cada vez que el usuario requiera llevar a cabo la recuperación de un memorándum	

Caso de Uso	BÚSQUEDA	
Acción	I. Acción “IMPRESIÒN”	
Descripción	Esta acción permitirá la impresión del memorándum	
Precondición	El usuario deberá estar dado de alta en el sistema. El usuario deberá estar logado en el sistema. El usuario deberá contar con un memorándum ya generado	
Secuencia normal	**Paso**	**Acción**
	1	El usuario ingresa al sistema para hacer la solicitud de imprimir un memorándum.
	2	Si el memorándum es privado. Excepción IMPRESIÓN
	3	El usuario solicita mediante la acción directa imprimir
Postcondición	Es responsabilidad del usuario que solicita la impresión del memorándum del contenido del mismo.	
Excepciones	**Excepción IMPRESIÓN**	
	Paso	**Acción**
	1	Si el documento a imprimir es privado, será necesario que el usuario tenga la llave privada para poder solicitar la acción de imprimir.
Frecuencia esperada	Cada vez que el usuario requiera llevar a cabo la impresión de un memorándum	
Importancia	Indispensable para contar con la presencia física de un memorándum.	

El caso de uso “setup” figura 3.9, se utilizará para hacer las configuraciones necesarias que el sistema requiera.

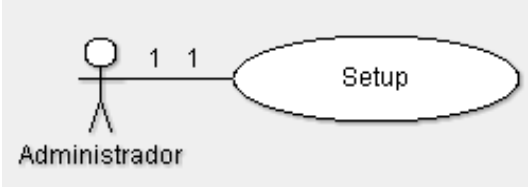

Figura 3.9 Diagrama Caso de Uso Setup

CAPÍTULO IV
WORKFLOW DEL ANÁLISIS Y DE DISEÑO

4.1 El Workflow del Análisis.

Durante el desarrollo del Workflow del análisis, se extraen las clases para obtener una comprensión más profunda de los requisitos. También se plasman los diagramas de secuencia para comprender la interacción de un conjunto de objetos en una aplicación a través del tiempo.

Una vez comprendidos los requisitos , se plasman en los diagramas de clases y de secuencia, con la finalidad de proponer un diseño para la arquitectura del sistema.

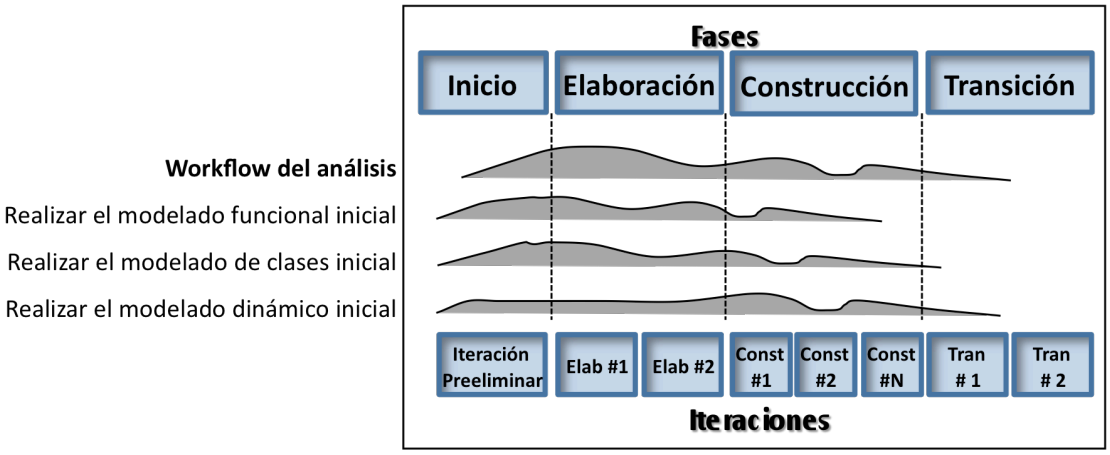

Figura 4.1 Diagrama RUP del Workflow del análisis.

4.1.1 Extracción de las clases entidad.

La extracción de las clases entidad véase, figura 4.2, consiste en tres pasos que se llevan a cabo de manera iterativa y por incrementos.

- Modelado funcional.- en él se presentan los escenarios de todos los casos de uso.
- Modelado de clases.- En él se determinan las clases y sus atributos, luego se definen las interrelaciones e interacciones entre las clases. Se presenta esta información en forma de un diagrama de clases.
- Modelo dinámico.- Se determinan las operaciones realizadas por o con cada clase o subclase.

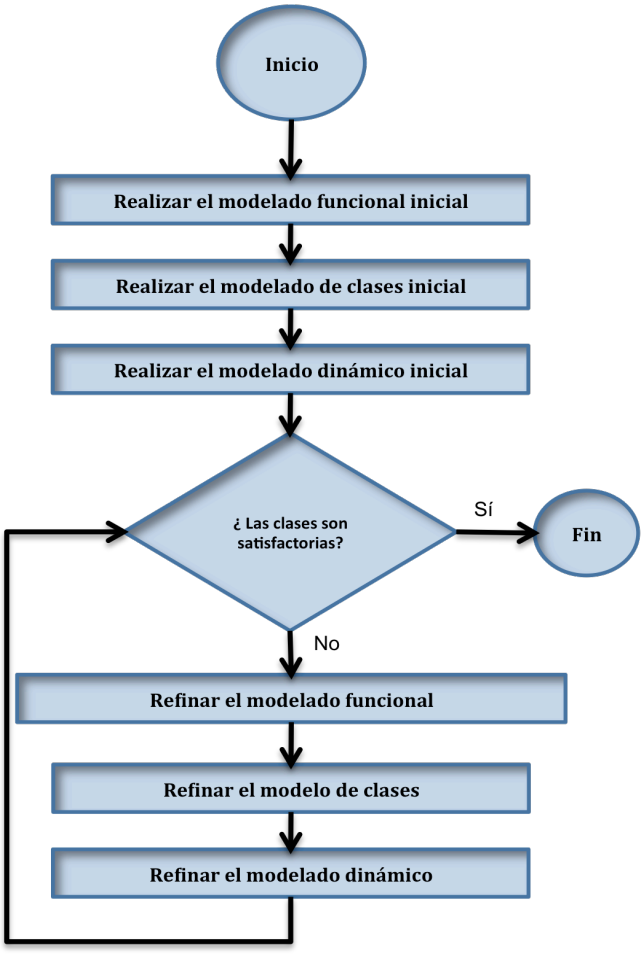

Figura 4.2 Diagrama de extracción de la clases entidad.

El resultado obtenido de la extracción de clases para el diseño del sistema de gestión de memorándums electrónicos, se muestra en el siguiente diagrama de clases, figura 4-3. Llamamos como clase principal a “sesión”, ya que de esta clase se van a deslindar la clase usuario, almacén, interfaz, dispatch y man, dentro de las cuales se plasman los requisitos funcionales que se obtuvieron en la fase del workflow de los requisitos.

En la clase “usuario” se establece que va a hacer uso de otras clases como lo son: la clase “cuenta”, “contraseña” y “pregunta clave” ya que estas contemplan parte del control de acceso que se va a tener en el sistema, en donde los usuarios van a tener un identificador de usuario y una contraseña para poder ingresar al sistema.

Por otra parte también en la clase de “usuario” se deslindan otras clases más como lo son: clase “perfil”, “rol”, “permisos”, estas se enfocan hacia la parte de permisos que van a tener los usuarios en el sistema según su perfil. El conjunto de estas nos lleva a la clase “colección de usuarios”, que es donde se va a tener el repositorio de los usuarios que fueron dados de alta en el sistema.

En la clase “interfaz vista”, “vista” y “elementos” van actuar en el sistema como un generador de interfaces para tener una interacción cliente-sistema.

En la clase “almacén” va almacenar los memorándums que fueron creados como se plasma en la clase “memo clear” y “memo signed”.

La clase “man” va a actuar como transaccional, ya que para que un usuario del sistema quiera efectuar alguna acción, ésta clase tiene que pedir a la clase “colección de usuarios” y/o a la clase “almacén” los datos necesarios para la ejecución de la acción solicitada.

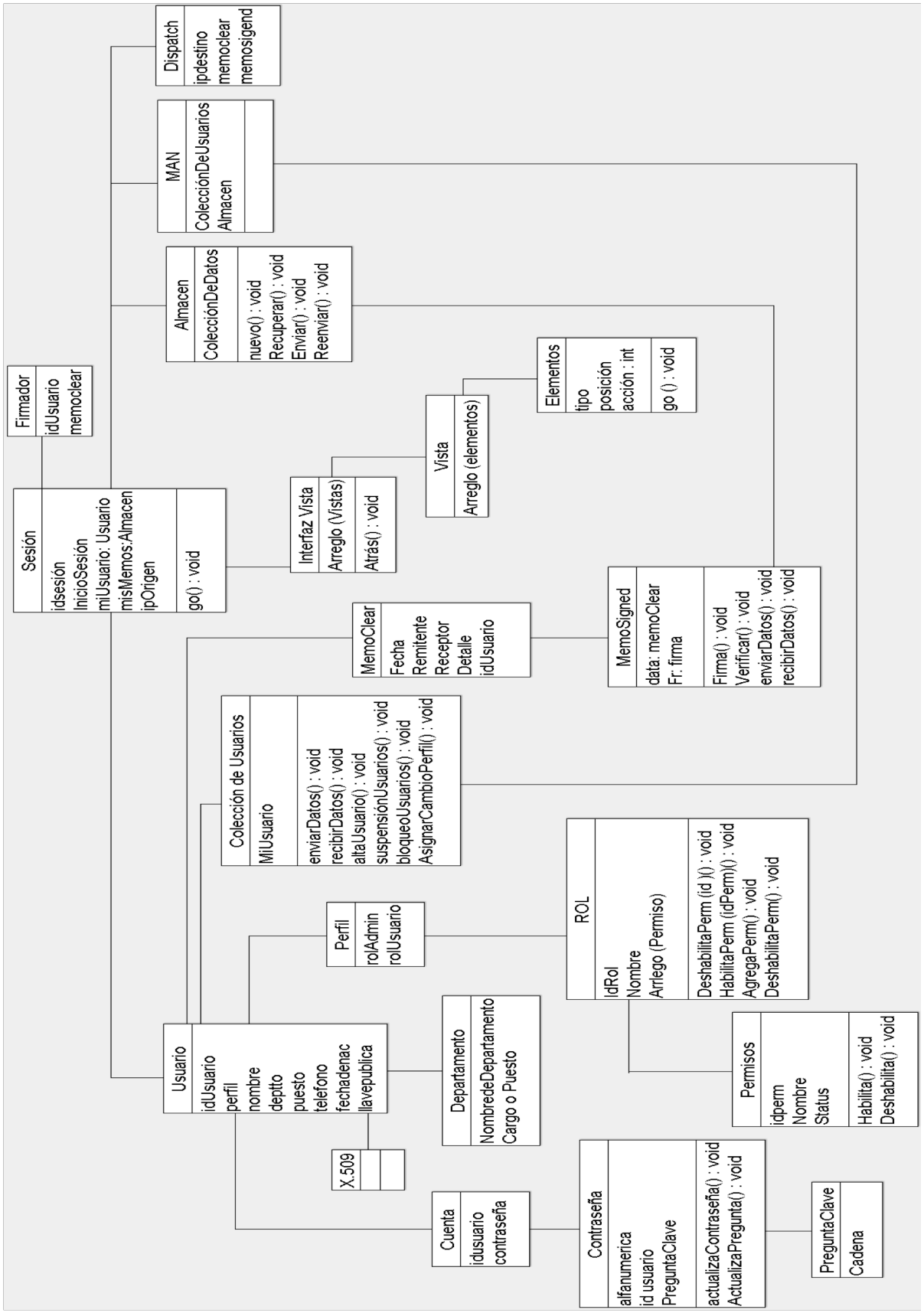

Figura 4.3 Diagrama de Clases

4.1.2 Diagramas de Secuencias

Retomando lo mencionado en el capítulo II, los diagramas de secuencia contienen detalles de implementación del escenario, incluyendo los objetos y clases que se usan para implementar el escenario y mensajes intercambiados entre los objetos.

Se podría decir que, se examina la descripción de un caso de uso para determinar qué objetos son necesarios para la implementación del escenario. Si se dispone de la descripción de cada caso de uso como una secuencia de varios pasos, entonces se puede "caminar sobre" esos pasos para descubrir qué objetos son necesarios para que se puedan seguir los pasos.

Un diagrama de secuencia muestra los objetos que intervienen en el escenario con líneas discontinuas verticales, y los mensajes pasados entre los objetos como flechas horizontales.

En los siguientes diagramas de secuencia de nuestro caso práctico, se muestran los objetos que intervienen y los pasos o camino a seguir, para que se pueda realizar cada acción.

Para poder llegar a estos diagramas de secuencia se examinó la descripción de un caso de uso (presentados en el capítulo III), y así determinar qué objetos eran los necesarios para la implementación del escenario.

Como por ejemplo, en este primer diagrama de secuencia llamado “alta” figura 4.4 nos muestra los objetos que intervienen (operador, sesión, interfaz de usuario, colección de usuario y man), y los pasos que se tienen que seguir para que se pueda realizar esta acción.

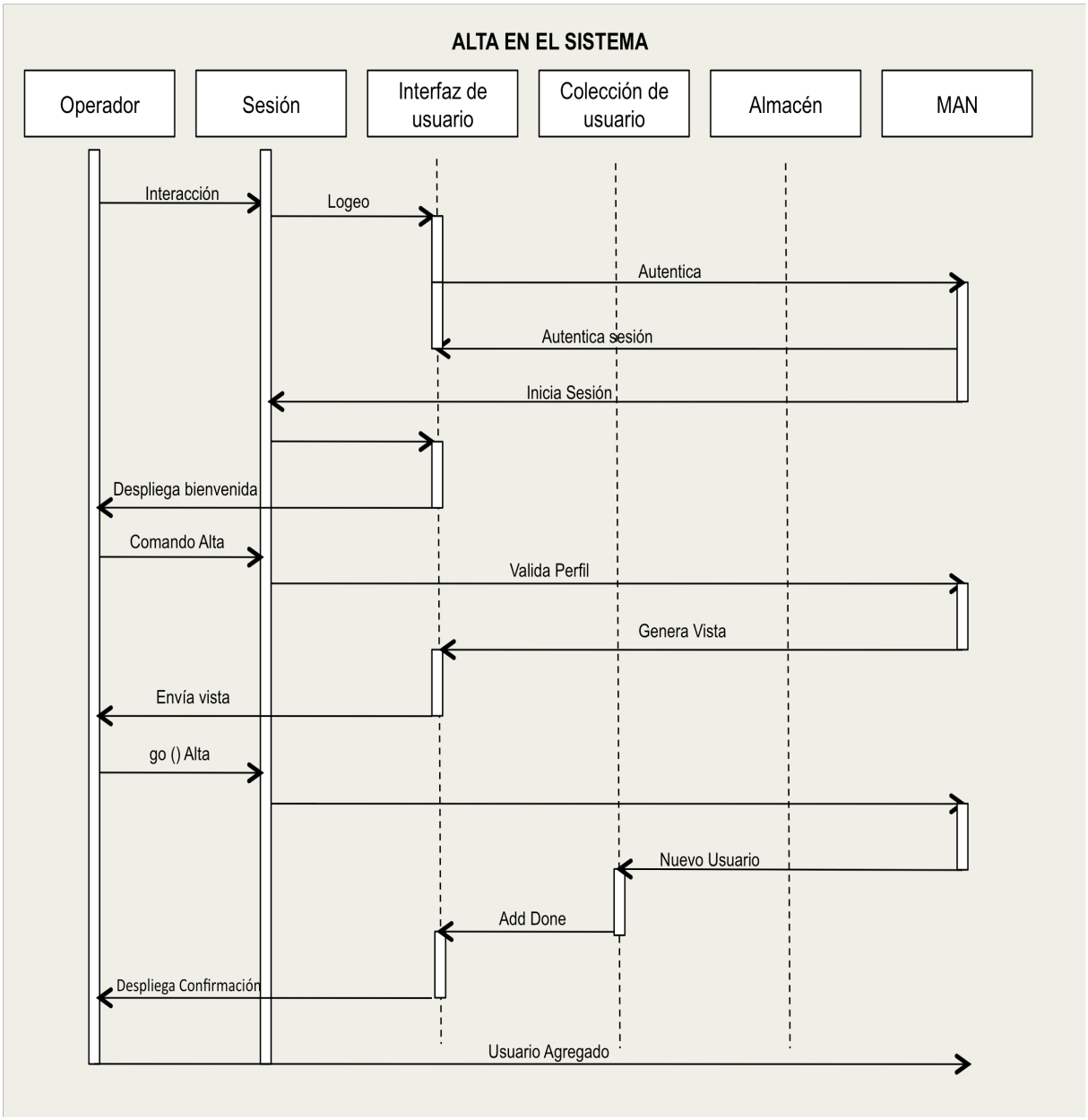

Figura 4.4 Diagrama de secuencia Alta en el Sistema

En este diagrama de secuencia “Login”, figura 4.5 se plasma los pasos a seguir para que el operador se pueda dar de alta en el sistema.

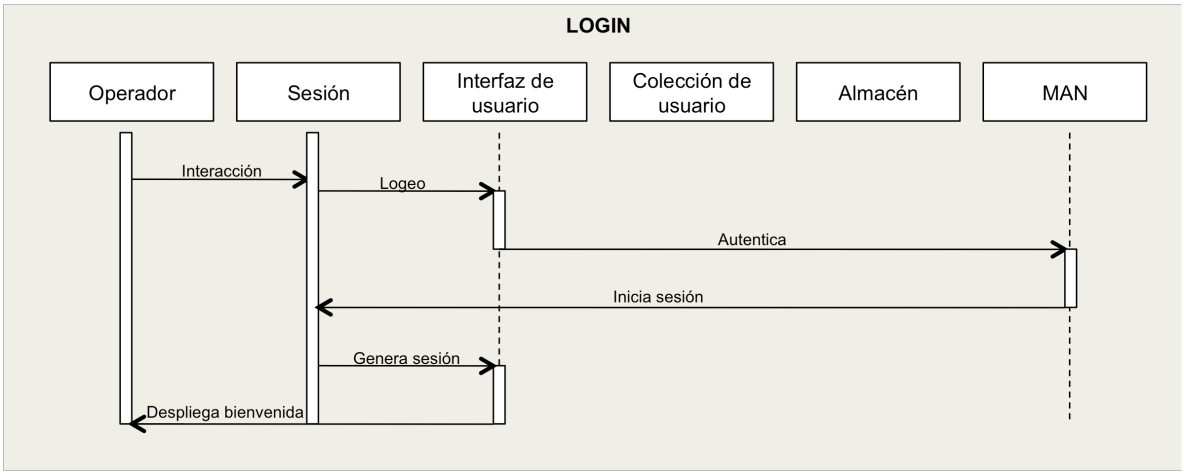

Figura 4.5 Diagrama de secuencia Login

El diagrama de secuencia, figura 4.6 representa los pasos a seguir para el Desbloqueo de Contraseña.

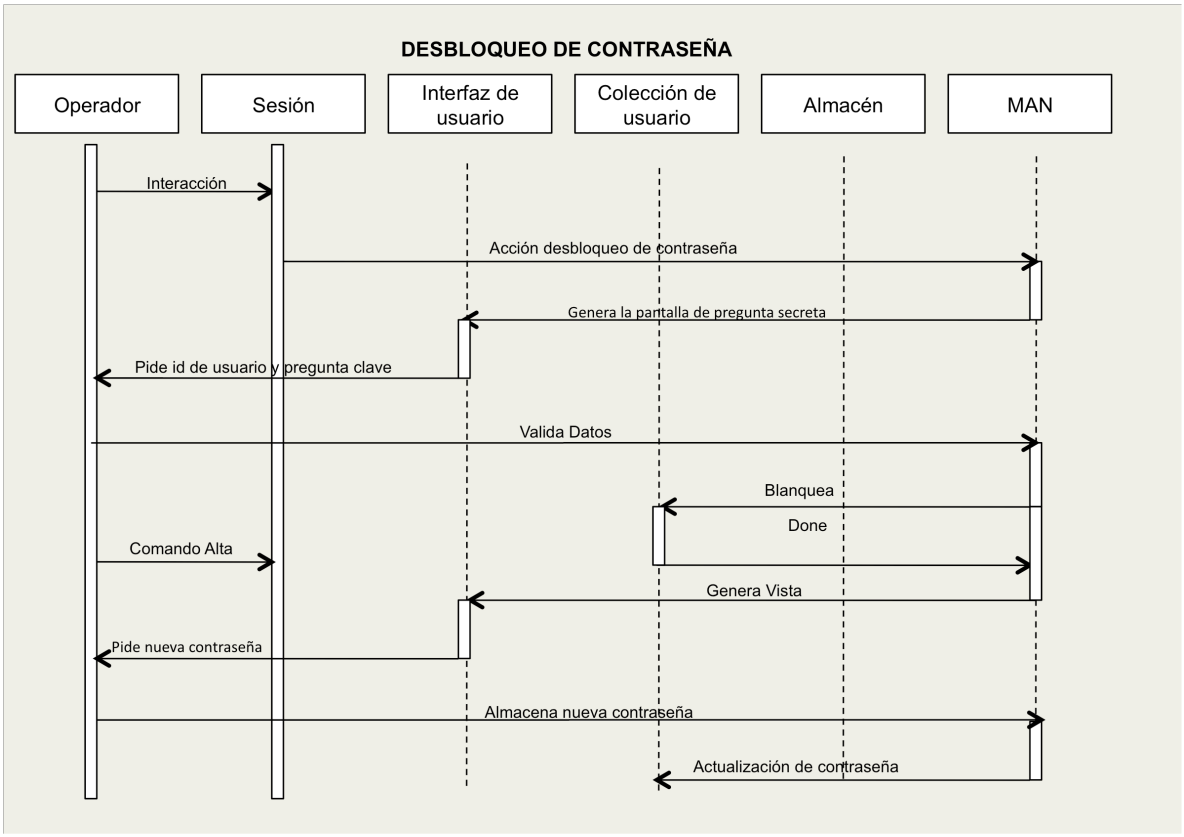

Figura 4.6 Diagrama de secuencia Desbloqueo de Contraseña.

El diagrama de secuencia, figura 4.7 representa los pasos a seguir para la Modificación de Contraseña.

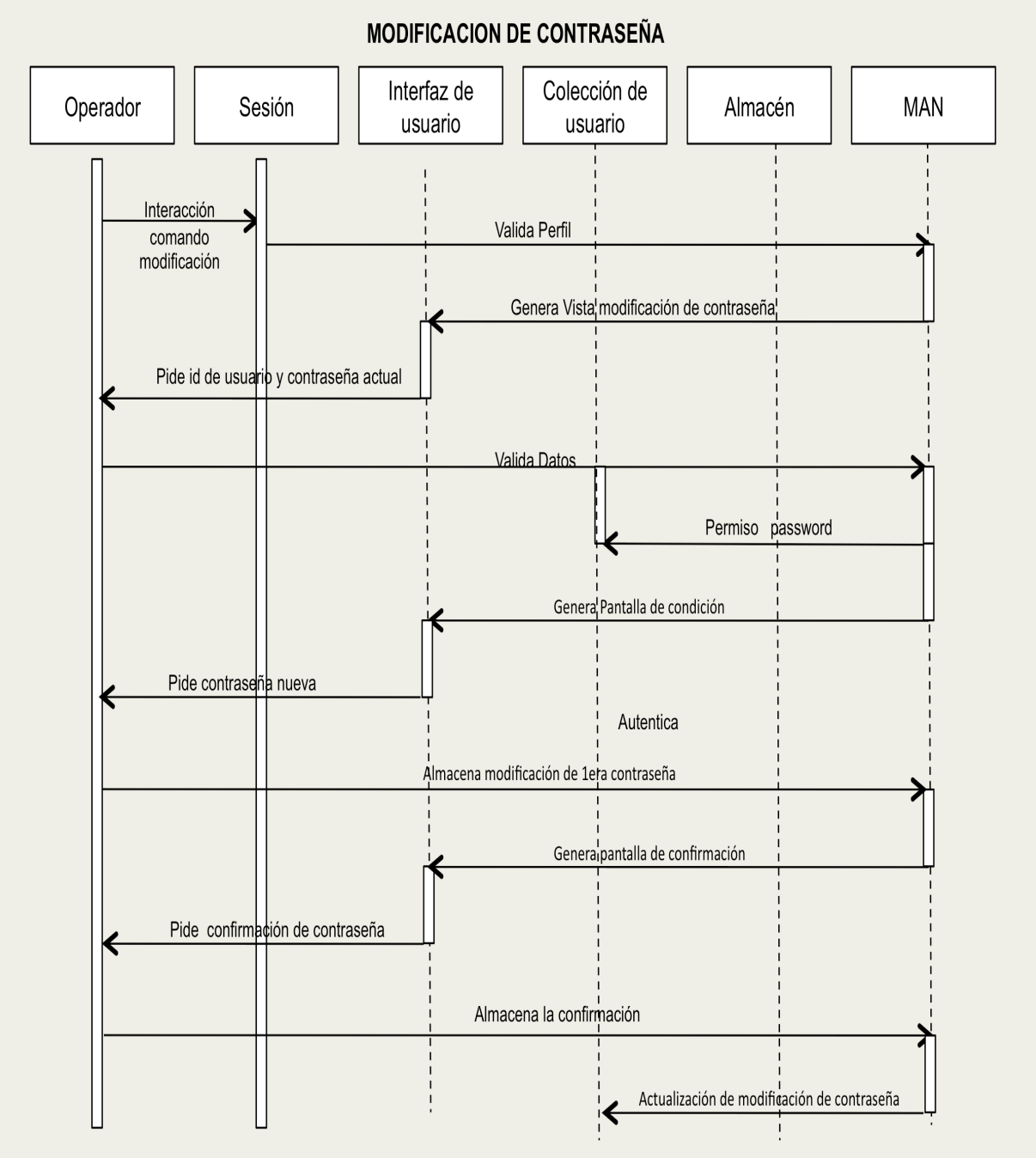

Figura 4.7 Diagrama de secuencia Modificación de Contraseña.

El diagrama de secuencia, figura 4.8 representa los pasos a seguir para la Suspensión de Usuario.

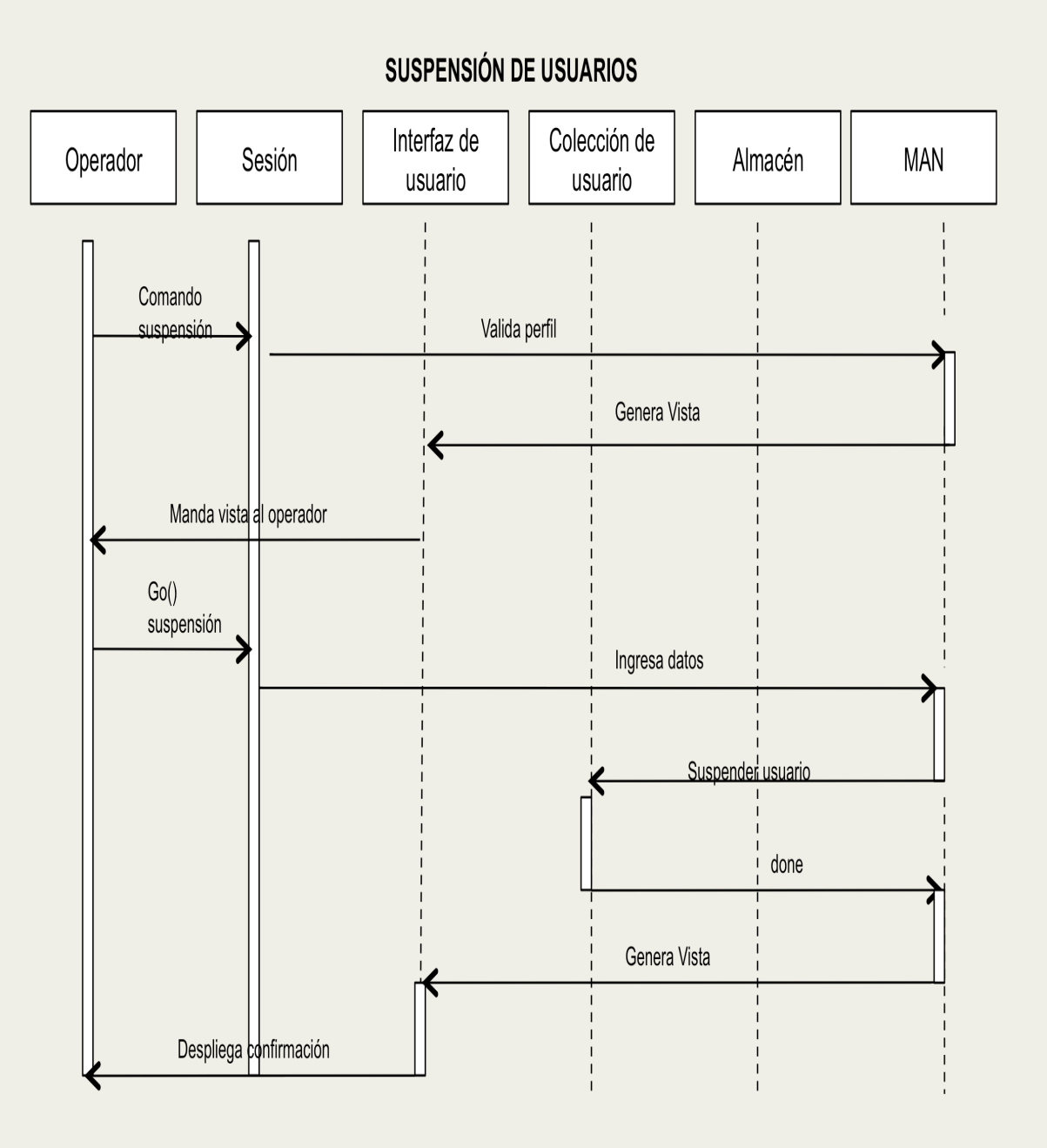

Figura 4.8 Diagrama de secuencia Suspensión de Usuarios.

El diagrama de secuencia, figura 4.9 representa los pasos a seguir para el Reset de Contraseña.

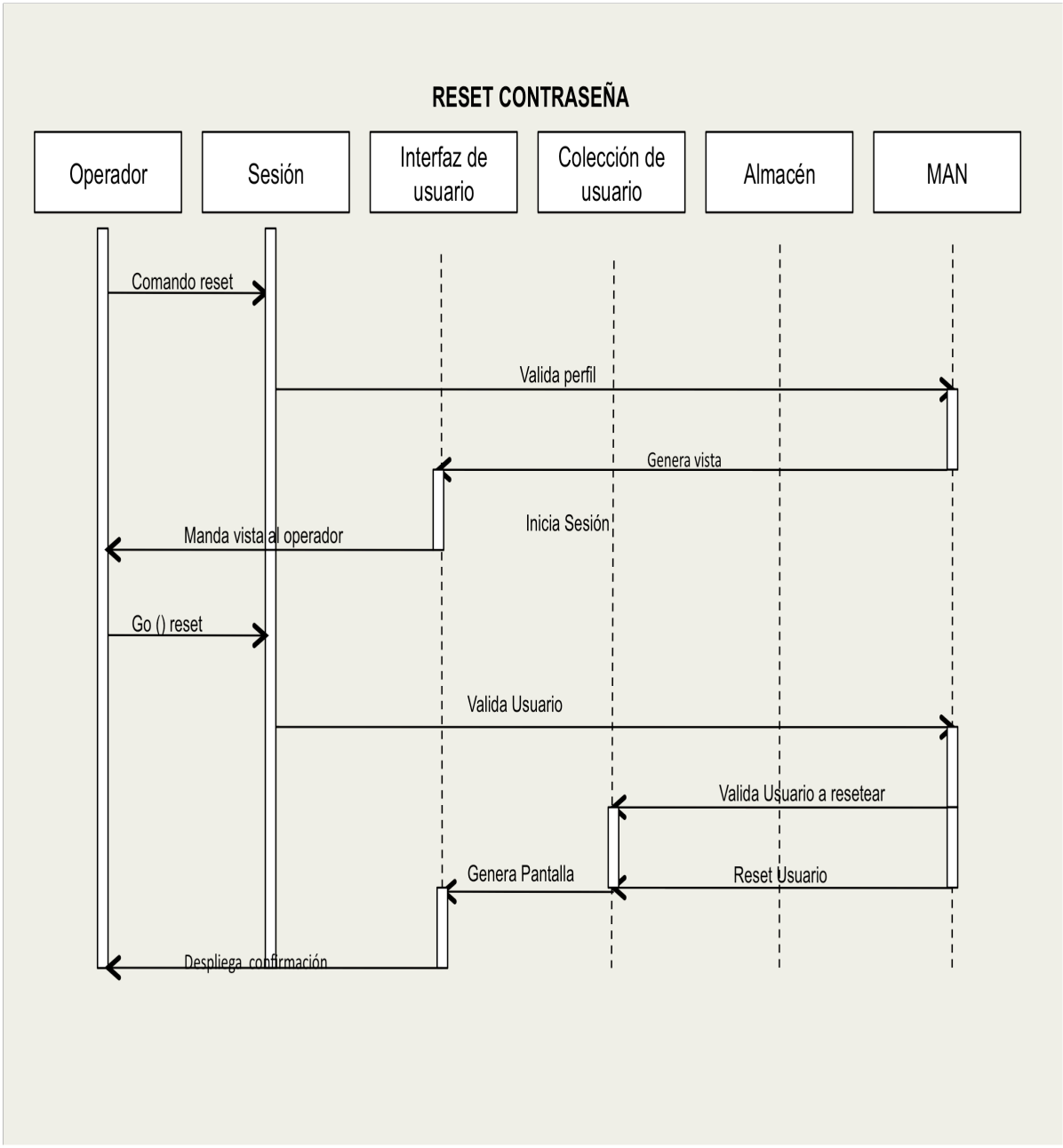

Figura 4.9 Diagrama de secuencia Reset Contraseña.

En este diagrama de secuencia llamado “generación” figura4.10, nos muestra los objetos que intervienen (operador, sesión, interfaz de usuario, colección de usuario, almacén y man), y los pasos que se tienen que seguir para que el usuario pueda generar un memorándum dentro del sistema.

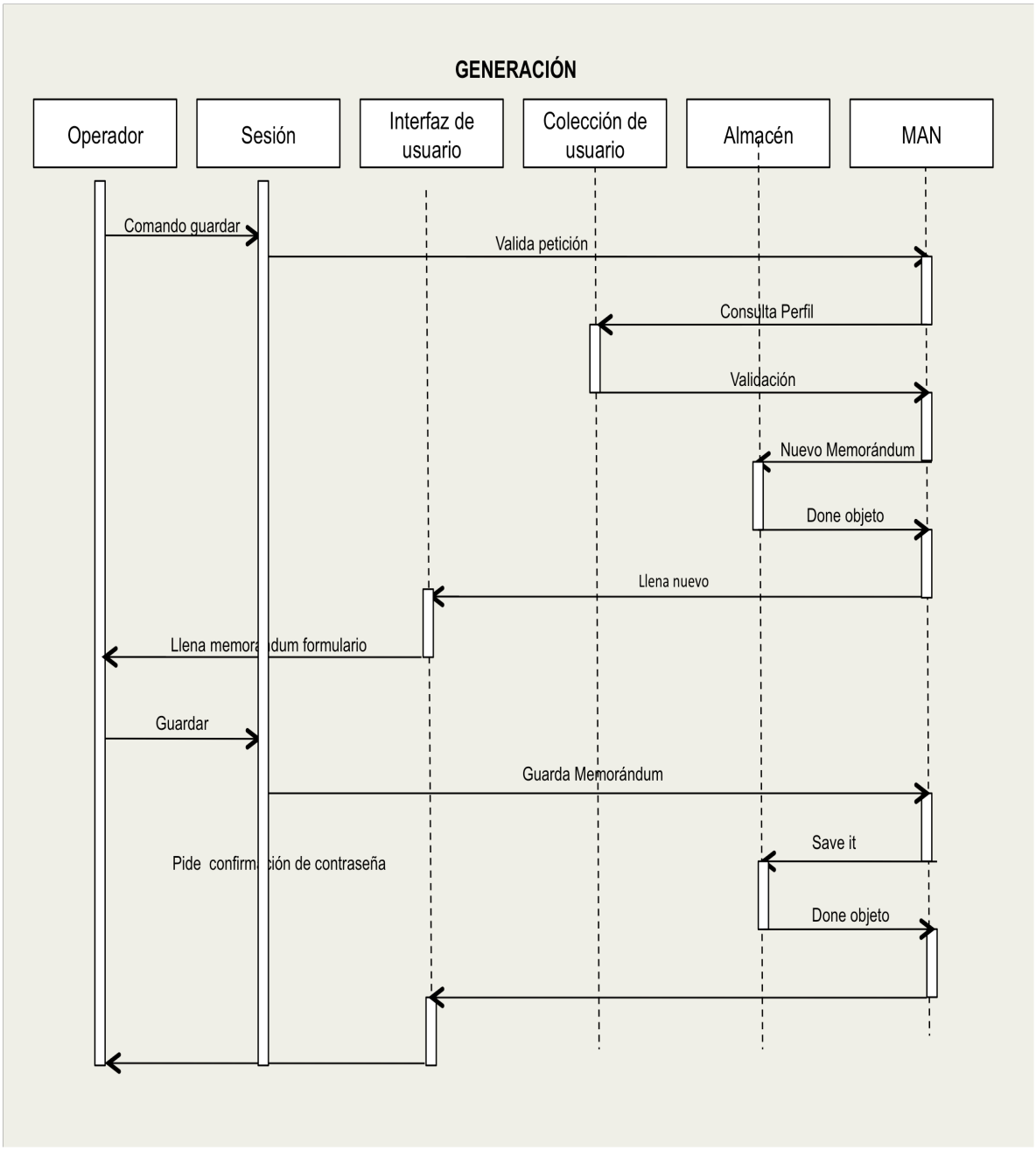

Figura 4.10 Diagrama de secuencia Generación.

En este diagrama de secuencia llamado “firma de memorándum” figura 4.11 para que se pueda mandar a pedir la acción de firmar, es necesario que con anterioridad se haya generado un memorándum.

Para que se pueda llevar a cabo esta acción es indispensable que exista un modulo de dispatch (despachador de firmas) y otro llamado firmador (este último no está considerado dentro del sistema), como se muestra en el diagrama.

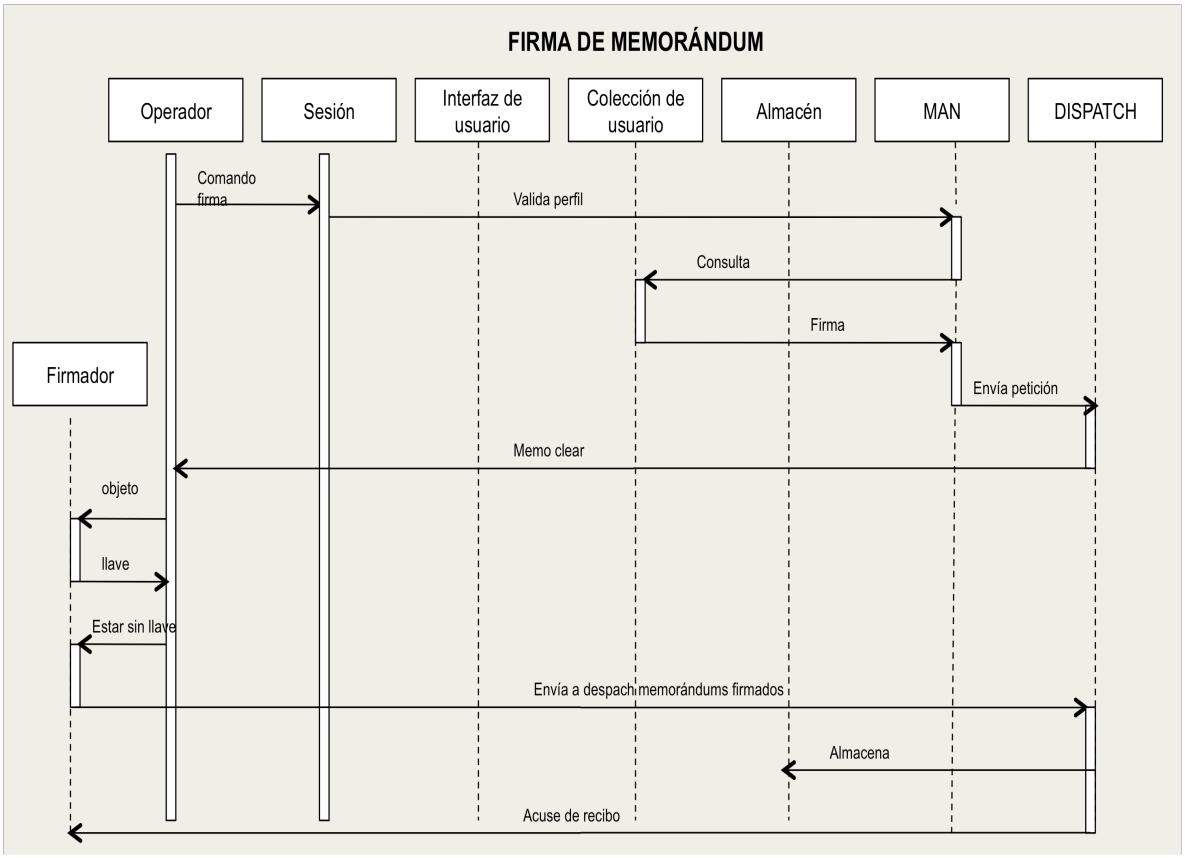

Figura 4.11 Diagrama de secuencia Firma de Memorándum.

Para que las acciones de los siguientes diagramas de secuencia (envío, reenvío, búsqueda, recuperación), se puedan llevar a cabo es necesario que haya un memorándum ya creado.

El diagrama de secuencia, figura 4.12 se representa los pasos a seguir para el proceso envío.

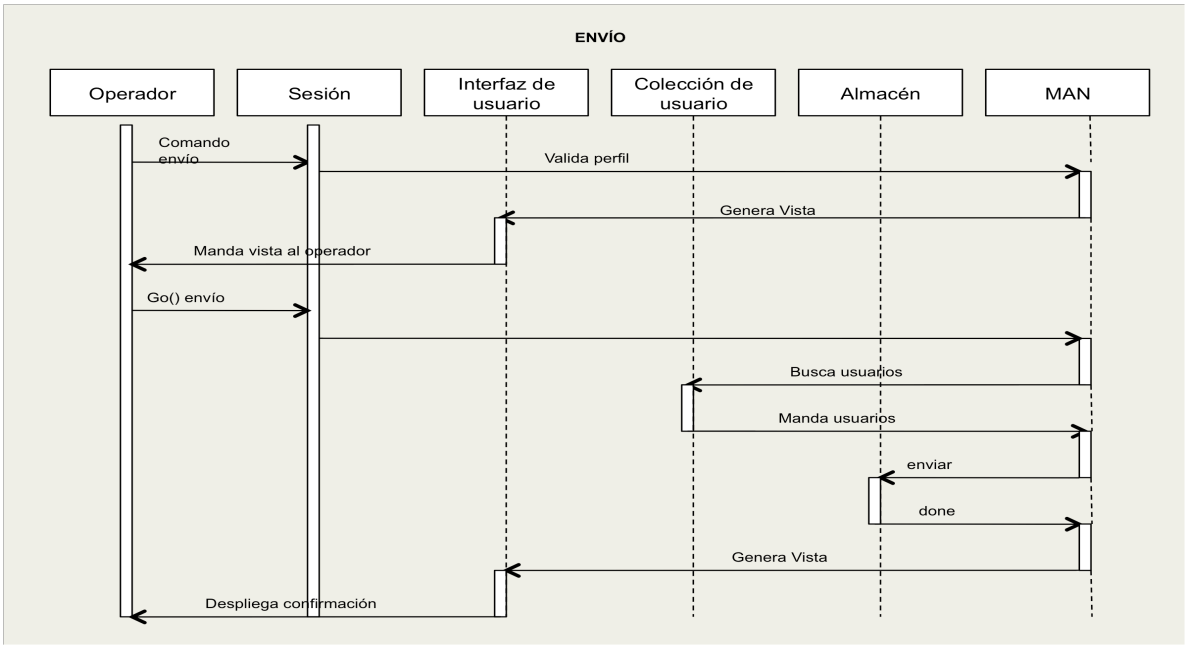

Figura 4.12 Diagrama de secuencia Envío

El diagrama de secuencia, figura 4.13 representa los pasos a seguir para el reenvío.

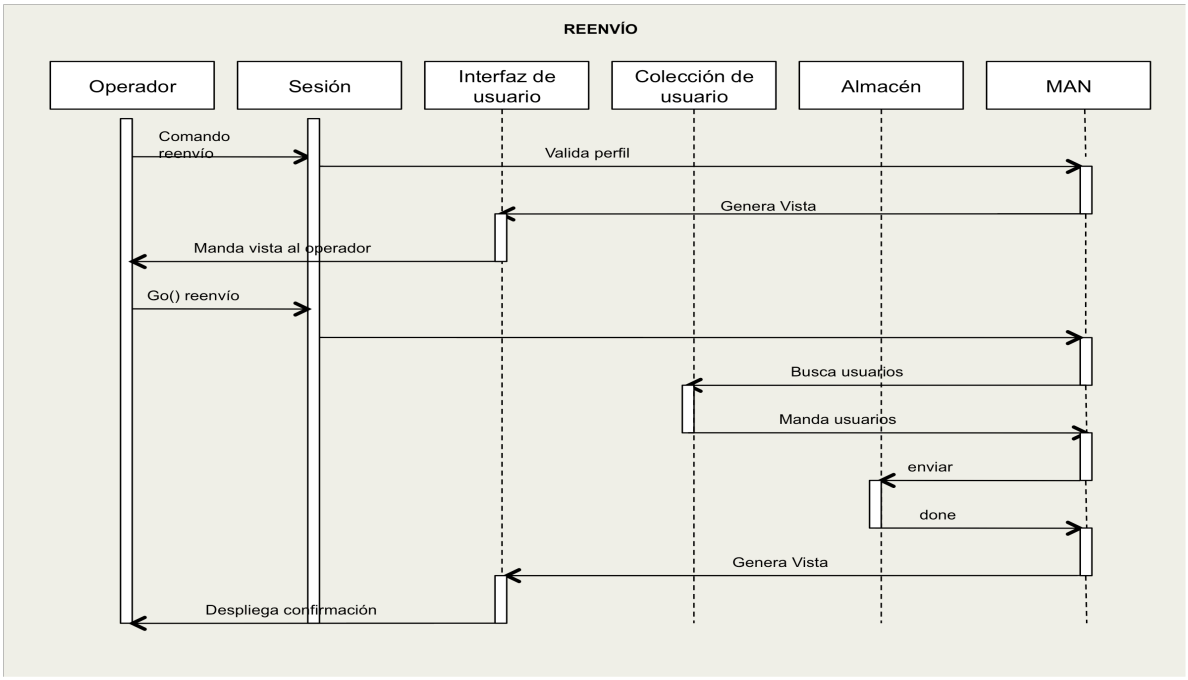

Figura 4.13 Diagrama de secuencia reenvío

El diagrama de secuencia, figura 4.14 representa los pasos a seguir para la Búsqueda.

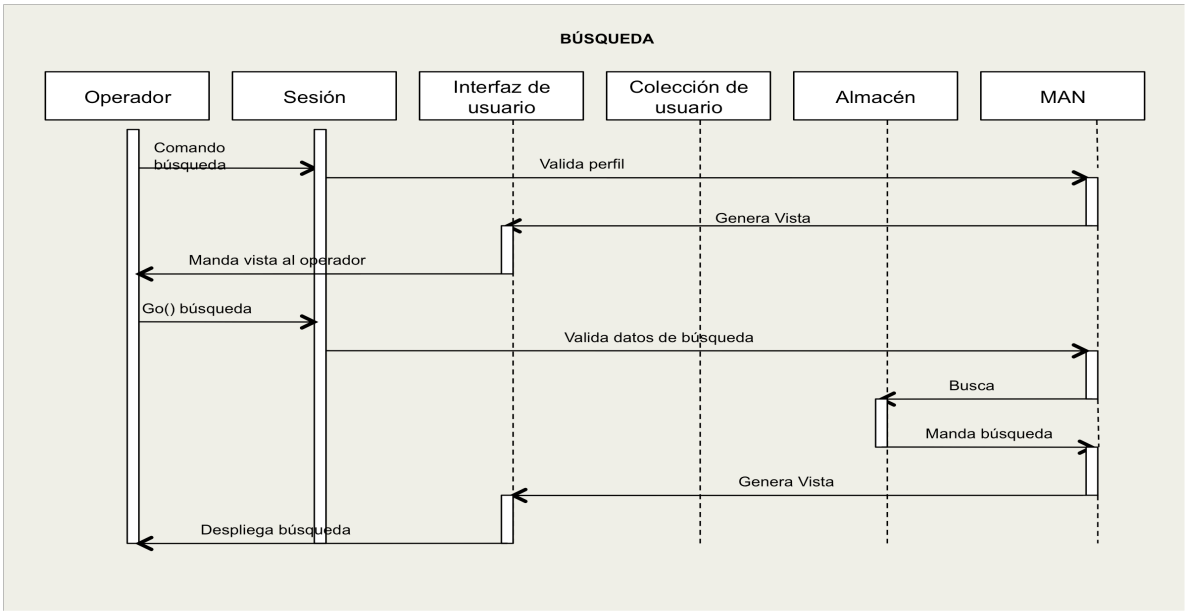

Figura 4.14 Diagrama de secuencia Búsqueda.

El diagrama de secuencia, figura 4.15 representa los pasos a seguir para la Recuperación.

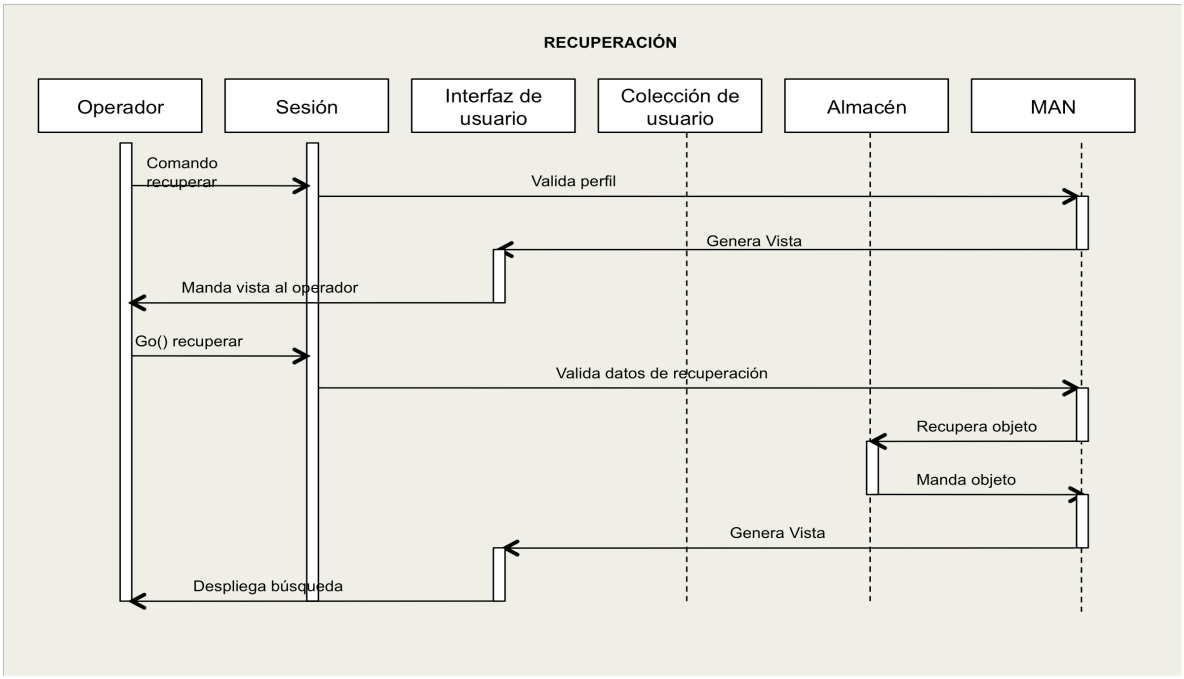

Figura 4.15 Diagrama de secuencia Recuperación.

4.2 El Workflow del Diseño

4.2.1 Arquitectura de los componentes

La arquitectura proporciona el vínculo entre la extracción de las necesidades del cliente, los componentes con los que dispone y su implementación.

En el diagrama de arquitectura propuesto, figura 4.16, se muestran los componentes y su interrelación; la aplicación se ejecutará en un ambiente web, por lo que uno de los requisitos para ejecutar el setup, es que los equipos de computo cuenten con acceso a la Internet, el cual funcionará como canal seguro de comunicación, dichos equipos deberán contar con servicios básicos de red (Internet), con los cuales si cuenta la ESIME.

El cliente ejecutará el sistema desde un equipo conectado a Internet, este proceso incluye 3 componentes:

Sesión: Guardan el estado de las conexiones

Interfaz gráfica de usuario: Mostrará la aplicación para ejecución del sistema.

Dispatch: Es una aplicación generadora de firma digital que será invocado solo durante el proceso de firmado.

Al estar dentro de una sesión y de acuerdo a los procesos seleccionados (casos de uso) se estará interactuando con:

Colección de Usuarios: Será un repositorio en el cual se almacenen todos los registros de usuarios

MAN.- Es un control de seguridad, que es un validador de transacciones.

Almacén.- Es el repositorio de memorándums

Estos componentes se propone que se encuentren almacenados en un repositorio de datos sobre un servidor de aplicaciones.

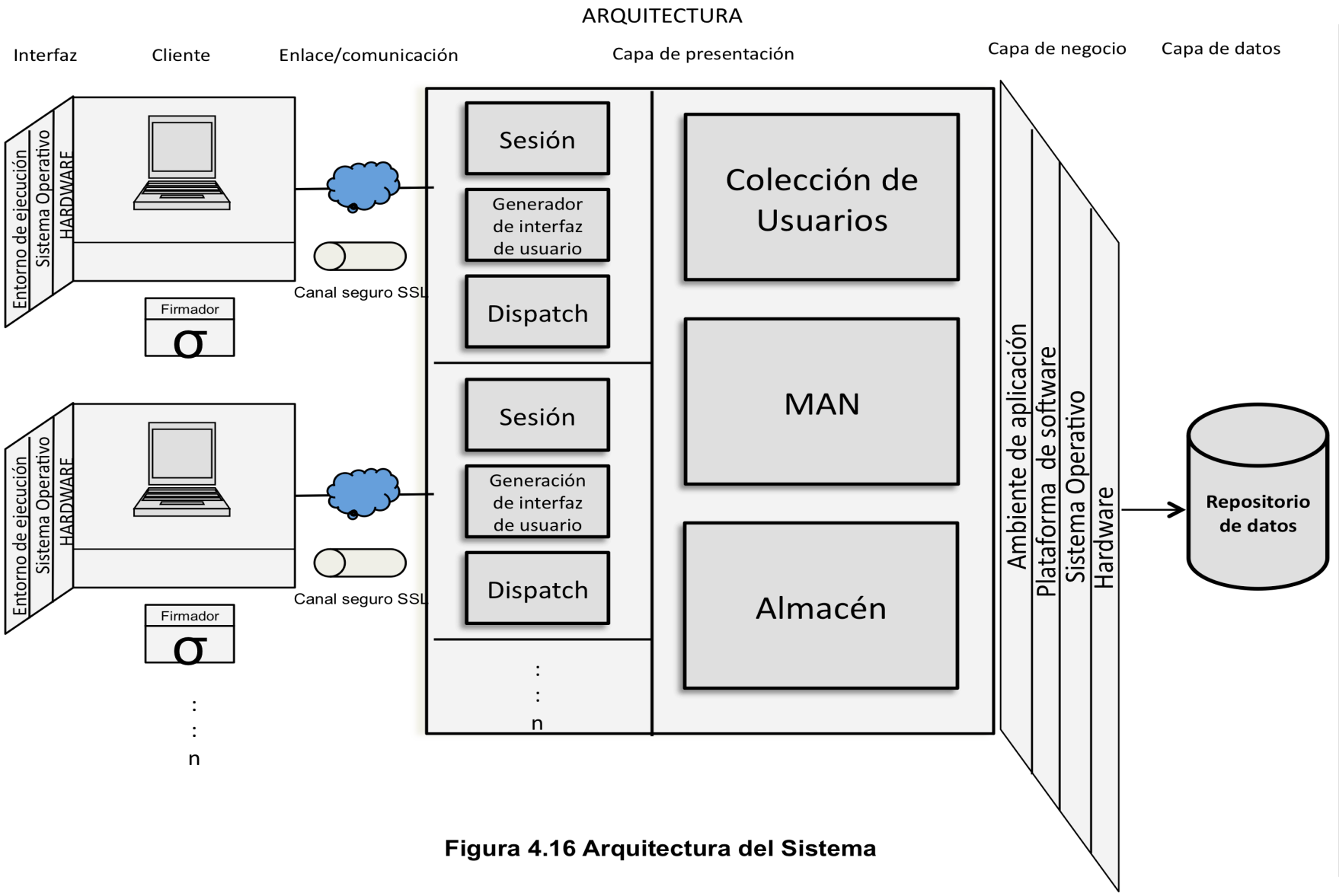

Figura 4.16 Arquitectura del Sistema

En el siguiente diagrama, figura 4.16 se resumen las actividades que se desarrollaron durante el desarrollo de nuestro diseño.

Fases

	Inicio	Elaboración	Construcción	Transición
Workflow de los requisitos	Se determinó y delimitó el alcance del proyecto. Se determinaron algunos requisitos preliminares.	Se realizaron cuestionarios a las áreas estratégicas, se analizaron y se obtuvieron los requisitos funcionales y no funcionales.	Durante el proceso se verificó que los requisitos no cambiaran y que los procesos se apagaran a los mismos.	Se verificó que el diseño entregado cumpla con los requisitos funcionales y no funcionales.
Workflow del análisis	Se comenzó a realizar el análisis de las casos de uso críticos involucrados en el proceso de gestión de memorándums dentro de la organización.	En base a los requerimientos funcionales se desarrollaron los casos de uso y haciendo uso de estos se realizaron los diagramas de clases y secuencia.	Se realizaron las correcciones detectadas en cada uno de los diagramas	Se realizan los cambios, si hay alguna falla o cambio que involucre el análisis.
Workflow del diseño	Se realizó un pre-diseño de la arquitectura basado en el análisis de la estructura de la institución.	Se realizó el refinamiento de la arquitectura básica de acuerdo a los requisitos no funcionales obtenidos.	Se entrega una propuesta de arquitectura terminada.	Se realizan los cambios, si hay alguna falla o cambio que involucre el diseño.
	Iteración Preeliminar	Elab #1	Elab #2	Const #1	Const #2	Const #N	Tran # 1	Tran # 2

Figura 4.16 Diagrama de Actividades Desarrolladas.

CONCLUSIONES

Se logró diseñar un sistema, con el cual el usuario es capaz de crear, intercambiar memorándums electrónicos mediante el uso de un método seguro, que permita agilizar tanto el acceso como garantizar la autenticidad y la recuperación de memorándums almacenados. Esto gracias a que se proponen medidas de seguridad como lo son un validador de transacciones (para prevenir que haya un manipulador de secuencias) y el uso de la firma digital, así como también hay que destacar que la clave privada se queda temporalmente en el servidor y una vez firmado se destruye.

Se logró identificar y comprender los requerimientos para el procesamiento de memorándums, así como el comprender y aplicar las metodologías RUP y el lenguaje de modelado UML

También se logró elaborar una propuesta para la arquitectura del sistema, en base a los requisitos no funcionales, obtenidos durante el desarrollo de nuestro proyecto.

Como conclusiones finales del proyecto se puede decir que se obtuvieron satisfactoriamente los resultados esperados, y se logró diseñar el sistema de gestión de memorándums electrónicos en la ESIME Culhuacan, con este nuevo diseño se plantea agilizar el proceso de gestión de los memorándums, así como garantizar la seguridad e integridad de los mismos.

GLOSARIO

ASIMÉTRICO: Es un método criptográfico que usa un par de claves para el cifrado de mensajes.

AUTENTICACIÓN: Es un método mediante el cual se asegura que los usuarios son quién dicen ser, que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacerlo.

CIFRADO: Es un método que permite implementar el servicio de seguridad de un mensaje o de un archivo mediante la codificación del contenido.

CONFIDENCIALIDAD: Protección de los datos contra la revelación no autorizada.

CRIPTOGRAFÍA: Es el estudio de técnicas matemáticas relacionadas a los aspectos de seguridad de la información como la confidencialidad, integridad de los datos, autenticación de la entidad, y autenticación de origen de los datos.

FIRMA DIGITAL: Es un control criptográfico primitivo, utilizado para garantizar autenticación, autorización y no repudio ante una tercera entidad.

HASH: Función que comprime la información en bloques de longitud fija.

HADWARE: Es cualquier componente físico tecnológico, que trabaja o interactúa de algún modo con la computadora.

MEMORÁNDUM: Escrito que se usa para intercambiar información entre diferentes departamentos de una empresa.

METODOLOGÍA: Ciencia de los métodos. // Manera de desarrollar un sistema de información.

NO REPUDIO: Protección contra la interrupción por parte de una de las entidades implicadas en la comunicación.

PARADIGMA: Modelo ó patrón // Se utiliza para referirse a un estilo de desarrollo de sistemas información.

PRIMITIVAS: Son la función más básica que compone un sistema criptográfico.

RUP: Proceso Unificado Racional.

SI: Sistema de Información.

SIMÉTRICO: Es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes.

SOFTWARE: Es todo programa o aplicación programado para realizar tareas específicas.

UML: Lenguaje Unificado de Modelado.

WORKFLOW: Flujos de Trabajo.

XOR: Es componente imprescindible en los circuitos sumadores de números binarios, tal como los utilizados en las calculadoras electrónicas.

REFERENCIAS

[1] http://es.wikipedia.org/wiki/Sistema_de_informaci%C3%B3n

[2] http://ayuda.fotopex.com/documentos/ejemplo-de-un-memorandum/

[3] http://www.contenidoweb.info/documentos/gestion-de-documentos.htm

[4] http://es.wikipedia.org/wiki/Gesti%C3%B3n_documental

[5] Stephen R. Schach, “Análisis y Diseño Orientado a Objetos con UML y el Proceso Unificado”

[6] http://biblioteca.usac.edu.gt/tesis/08/08_7691.pdf

[7] Grady Booch James R. Ivar Jacobson “El Lenguaje Unificado de Modelado”

[8] http://computacion.cs.cinvestav.mx/~jjangel/todos/firma_digital.pdf

[9] http://es.wikipedia.org/wiki/Sistema_de_informaci%C3%B3n

[10] http://elvex.ugr.es/decsai/java/pdf/3E-UML.pdf

BIBLIOGRAFÍA

- Stephen R. Schach, “Análisis y Diseño Orientado a Objetos con UML y el Proceso Unificado”.
- Grady Booch James Rumbaugh Ivar Jacobson “El Lenguaje Unificado de Modelado”.
- Ingeniero Especialista Simon Pedro Torres, tesis sobre “Firma Digital 2009”.

ANEXO

CUESTIONARIO PARA LA CEGET

AREA: Coordinación de Enlace y Gestión Técnica

ENTREVISTADO: M. en C. Rosa E. Loya Lugo

CARGO: Jefa de la Coordinación de Enlace y Gestión Técnica

1.- ¿Qué es un memorándum?

Es el documento redactado en forma breve, relacionado con un asunto específico, el cual es emitido al interior de la unidad

2.- ¿Cuáles son los componentes básicos de información que contienen sus memorándums?

- leyenda memorándum
- fecha
- servidor a quien va dirigido precedido por la expresión “Para”

- puesto del servidor a quien va dirigido
- nombre del que suscribe el memorándum precedido por la expresión “De”
- puesto de quien emite el memorándum
- redacción en forma breve
- al termino del memorándum se anota la expresión “Atentamente”
- las abreviaturas c.c.p.

3.- ¿Cuentan con un formato específico para la creación de memorándums?

Si

4.- ¿Cómo se desarrolla la emisión, transmisión, recepción y acuse de recibo de los memorándums?

Se elabora el memorándum, se envía con el mensajero al destinatario, se entrega y el área sella de recibido

5.- ¿Cualquier persona tiene facultad para firmar un acuse de recibo?

No, solo el personal adscrito al área correspondiente

6.- ¿Cuál es el proceso que se lleva a cabo para el proceso de archivo de memorándums?

Los acuses se archivan de acuerdo al área que corresponden

7.- ¿Cualquier persona puede solicitar la consulta o duplicado de algún memorándum?

No, solo el funcionario responsable del área

8.- ¿Los formatos que utilizan para la creación de los memorándums, es autorizada por alguna área en especifico?

No, es responsabilidad de cada área

9.- ¿Cuánto tiempo que lleva aproximadamente la creación y entrega de un memorándum?

Ambas acciones se realizan en forma inmediata

10.- ¿Qué tipo de información se considera confidencial y sea turnada bajo firma con carácter de memorándum?

La información confidencial es aquella relativa a los datos personales y no se maneja en formato de memorándum, de acuerdo a los Fundamentos de los Archivos y la Administración de documentos (IFAI).

11.- ¿Los formatos que utilizan para la creación de los memorándums, es autorizada por algún área en específico?

De acuerdo a las necesidades y la información que requiera se manejan dos tipos de memorándums, el impreso y el electrónico, por lo que no existe estimación de la cantidad usada

12.- Aproximadamente, ¿Qué cantidad de papel es destinado anualmente para la impresión de memorándums?

No se cuenta con desperdicio de papel ya que esta área los utiliza para borradores de documentos.

Nota: Todo memorándum debe llevar un número de consecutivo, con las siglas del departamento y el año, ejemplo del departamento de ingeniería en Computación.

DIC/123/10

Donde DIC= Departamento de Ingeniería en Computación

123= Al consecutivo del memo

/10= es el año.

Por último es importante aclarar que el memo con la firma autógrafa original es entregado al área “Para” y las áreas con la leyenda c.c.p. (con copia para) se les entregan los memos con facsímil y todos deberán ir sellados.

En todas las áreas el personal secretarial lleva un listado que se conoce como consecutivo de memos donde se escribe el nombre del área a donde va dirigida el número de consecutivo el asunto y la persona que lo elaboró, y de igual manera para el acuse se tiene un formato con los mismos datos solo que ahora cambia el de la persona que lo elaboro por el de la persona que lo recibió.

CUESTIONARIO PARA JEFE DE OFICINA O REPRESENTANTE

AREA: Departamento de Investigación.

ENTREVISTADO: Ing. Enrique Escamilla Hernández.

CARGO: Jefe del Departamento de Investigacion.

1.- ¿Utilizan algún mecanismo de control e integridad de firma autógrafa si es así cuáles son?

Firma autógrafa

2.- ¿Conoce algún mecanismo de firma digital?

El que más conozco es el de CONACyT, entre otros el CHASE, Bank of America y el de la función pública.

3.- Si es que conoce alguno de ellos… ¿Qué tan confiable considera que sea utilizar este mecanismo?

Considero que si han de ser muy confiables.

4.- ¿Existe alguna figura del fascimil para la firma de los memorándums, si es así, cuál es y cómo la manejan?

El fascimil solo se usa en copias, más no en el original.

5.- ¿Cualquier persona tiene facultad para firmar un acuse de recibo?

Sí

6.- ¿Se lleva algún registro de los memorándums enviados y recibidos?

Si, se lleva un número consecutivo y se maneja en una bitácora.

7.- ¿Cómo identifica a la persona que hace entrega de los memorándums?

No se identifica, es indistinto.

8.- ¿Cómo se identifica a las personas que participan en la elaboración de un memorándum redactor, revisor, visto bueno y remitente?

No lo hay

9.- ¿Cuánto tiempo es almacenada la información?

No sé cuanto sea el tiempo.

10.- ¿Se realiza alguna auditoria para garantizar la autenticidad de la información contenida, así como de la firma plasmada en los memorándums?

No.

CUESTIONARIO DE TI

ÁREA: Unidad de Informática

ENTREVISTADO: Miguel Ángel Juárez Hernández

CARGO: Jefe de la Unidad de Informática

1.- ¿Sobre qué plataforma trabajan los equipos?

Windows

2.- ¿Qué especificaciones de hardware tienen los equipos?

Intel Core Dos 3.0 GHz, 2GB en Ram, 250 GB

3.- ¿Qué especificaciones de software tienen los equipos?

Windows XP, Windows Vista, Windows 7, Office 2007, Visual Studio

4.- ¿Cuenta con alguna conexión a Internet?

SI

5.- ¿Qué tipo de conexión utilizan para Internet?

STM1

6.- ¿Con cuántos servidores de aplicaciones cuenta la red de la ESIME?

Uno (SAES)

7.- ¿Actualmente se maneja alguna aplicación de Intranet?

No

8.- ¿Cuál es el motivo de contar o no contar con ella?

No se ha planeado un proyecto en forma para implementarlo