UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía, las Industrias y los Recursos Naturales no Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

"DISEÑO Y CONSTRUCCIÓN DE UN SISTEMA AUTOMATIZADO PARA LA GESTIÓN DE DOCUMENTOS EN LA ILUSTRE MUNICIPALIDAD DEL CANTÓN CALVAS UTILIZANDO CERTIFICADOS DIGITALES"

Tesis previa la obtención del título de Ingeniero en Sistemas

AUTORES:

Patricia Elizabeth Chamba Briceño

Franklin Freddy Andrade Alverca

DIRECTOR:

Ing. Luis Antonio Chamba Eras

LOJA - ECUADOR

2010

Certificación:

Ing. Luis Antonio Chamba Eras
Catedrático de la Universidad Nacional de Loja y Director de la presente tesis

CERTIFICA:

Que, el proyecto de tesis titulado "DISEÑO Y CONSTRUCCIÓN DE UN SISTEMA AUTOMATIZADO PARA LA GESTIÓN DE DOCUMENTOS EN LA ILUSTRE MUNICIPALIDAD DEL CANTÓN CALVAS UTILIZANDO CERTIFICADOS DIGITALES" ha sido elaborado por la Srta. Patricia Elizabeth Chamba Briceño y el Sr. Franklin Freddy Andrade Alverca, previa la obtención del título de Ingeniero en Sistemas, revisado y corregido bajo mi dirección. Por lo tanto autorizo proseguir con los trámites legales pertinentes para su presentación y defensa.

Loja, Julio del 2010

……..
Ing. Luis Antonio Chamba Eras
DIRECTOR DE TESIS

Autoría

Las opiniones, ideas y conceptos suscritos en el presente proyecto de tesis, son de exclusiva responsabilidad de sus autores, restringiendo la copia, uso o utilización del sistema informático o documento de tesis sin autorización

…… ……

Patricia Elizabeth Chamba Briceño *Franklin Freddy Andrade Alverca*

Pensamiento

Los obstáculos son esas cosas que las personas ven cuando dejan de mirar sus metas.

E. Joseph Cossman

El logro es, ante todo, el producto de la constante elevación de nuestras aspiraciones y expectativas

Jack Nicklaus

Dedicatoria

En primer lugar a Dios por ser mi guía y compañero, de igual manera a mis padres y hermanos quienes en todo momento me apoyaron y animaron depositando su entera confianza en cada reto que se me presentaba, sin dudar ni un solo momento en mí y en mi capacidad. A todos ustedes mil gracias porque su apoyo fue la luz que me permitió llegar a la consecución de este gran logro académico.

Patty

A mi querida mamá Lucia, que con su amor, cariño, paciencia, apoyo y consejos me han enseñado a seguir luchando y venciendo las condiciones más difíciles de la vida.

A mi querida hermana y hermanos que siempre estuvieron ahí, amigos y amigas verdaderos. A todos ellos que han sido un apoyo incondicional en la culminación de una de mis metas.

Frank

Agradecimiento

Muchas han sido las personas que de manera directa o indirecta han participado en la realización de esta tesis por ello queremos agradecer su colaboración

Agradecemos primeramente a Dios por ser nuestro mejor amigo, nuestra fortaleza, por darnos todo lo que tenemos, por permitirnos llegar donde hoy estamos, y brindarnos una vida llena de experiencias enriquecedoras.

A nuestros padres quienes han sido un apoyo moral y económico para lograr este fin, Gracias por su paciencia

Al Ingeniero Luis Antonio Chamba Eras, asesor de tesis por ayudarnos a lo largo del presente trabajo, compartir su conocimiento con nosotros y acompañarnos en este camino que hoy culmina en el presente proyecto.

A la Universidad Nacional de Loja, al Área de la Energía, las Industrias y los Recursos Naturales No Renovables, a través de la Carrera de Ingeniería en Sistemas, donde obtuvimos los conocimientos técnicos que han contribuido a nuestra formación profesional

Un agradecimiento muy especial, al Gobierno Autónomo Descentralizado del Cantón Calvas, por habernos proporcionado valiosa información para realizar nuestro trabajo de tesis.

Finalmente, agradecemos a nuestros amigos y compañeros, porque la constante comunicación con ellos ha contribuido en gran medida a transformar y mejorar especialmente a aquellos que nos brindaron cariño, y comprensión, dándonos con ello, gratos momentos.

En general quisiéramos agradecer a todas y cada una de las personas que han vivido con nosotros la realización de esta tesis, con sus altos y bajos y que no necesitamos nombrar porque tanto ellas como nosotros sabemos que desde lo más profundo de nuestro corazón les agradecemos el habernos brindado todo el apoyo, colaboración, ánimo y sobre todo amistad.

Los Autores

2. RESUMEN

Hoy en día la seguridad de la información cumple un rol muy importante en cualquier institución, por tal motivo es que resulta necesario el utilizar estrategias encargadas de proteger tanto su contenido como su acceso.

El sistema automatizado para la gestión de documentos en la Ilustre Municipalidad del cantón Calvas utilizando certificados digitales, se desarrolló con la finalidad de permitir el envío y recepción de información de manera segura y confiable entre los diferentes departamentos que conforman esta institución. Para cumplir con tal efecto fué necesario el uso de certificados digitales generados por medio del algoritmo RSA. Cada certificado dispone de un par de claves denominadas: pública y privada respectivamente, mismas que le corresponderán a un solo usuario y que también serán las encargadas de permitir firmar digitalmente la información, de igual manera cabe señalar que se utilizó funciones hash.

Una función hash es una operación que da como resultado otro conjunto de datos, denominado resumen, que tiene la propiedad de estar asociado unívocamente a los datos de origen, valores que permitirán comprobar la autoría del mensaje enviado por el destinatario y recibido por su receptor.

Por lo antes indicado, un usuario será capaz de recibir información firmada digitalmente siempre y cuando disponga de un certificado digital activo, cuyas claves le permitirán verificar la autenticidad de la información recibida.

La presente aplicación, lo que busca es que reducir el tiempo de tramitación de un documento, así como también el garantizar seguridad en el acceso y envío de información.

SUMARY

Now days information security plays a major role in any institution for that reason is that it is necessary to use strategies involved in protecting both its content and access.

The automated system for records management in the Municipality of the city Calvas, using digital certificates, was developed in order to allow sending and receiving information securely and reliably between the different departments that make up this institution. To fulfill this purpose was necessary to use digital certificates generated by the RSA algorithm. Each certificate has a key pair called: public and private respectively, same as it will correspond to a single user and that will also be responsible for allowing the information digitally sign, just as it should be noted that hash functions are used or summary.

A hash function is an operation that results in another data set, called sum, which has the property of being uniquely associated with the source data, values order to verify the authorship of the message sent by the recipient and received by the receiver.

As indicated above, a user will be able to receive digitally signed information provided you have a digital certificate asset whose keys will allow you to verify the authenticity of the information received.

This application, which is seeking to reduce the processing time of a document, as well as to guarantee secure access and delivery of information.

3. INDICE

CONTENIDO *Pag*

INDICE DE TABLAS

CONTENIDO *Pag*

INDICE DE FIGURAS

CONTENIDO *Pag*

4. INTRODUCCIÓN

Hoy día estamos viviendo en la era de la revolución de la información. Todos necesitamos de la información para poder llevar a cabo las transacciones comerciales y personales. En esta era de avances tecnológicos, la información puede ser conseguida a través de diferentes medios como: el papel, los discos duros, cds y otros medios.

Cada día la mayoría de empresas se están dando cuenta de la necesidad de utilizar algún tipo de software, el cual debe estar enmarcado principalmente en el mejoramiento de su administración y prestación de servicios, esto con la finalidad que el control de la información se facilite considerablemente.

Es importante contar con un buen sistema de administración de documentos para poder almacenar y recuperar la información. Los documentos son un recurso y activo organizacional. Como recurso, proveen información y como activo, proveen documentación. Si utilizamos sistemas automatizados para archivar la información, éstos nos ayudan a localizar el documento en una forma más rápida y de igual manera si necesitamos enviar algún tipo de información dentro de la empresa lo podemos lograr de una manera veraz y oportuna.

Todo lo anterior hace necesario que las empresas utilicen sistemas seguros tanto para el envío como para la recepción de datos. Para ello resulta útil la encriptación y autenticación de los mismos; proceso que se consigue con el uso de certificados digitales, que permiten enviar y recibir información firmada digitalmente entre uno y varios usuarios, de manera rápida y con la seguridad de que el destinatario será el único que tendrá acceso a su contenido es decir llegará íntegra a su destino.

El Ilustre Municipio del cantón Calvas en la actualidad no dispone de un sistema automatizado encargado de la gestión documental, caracterizado principalmente por el envío y recepción de información entre los diferentes departamentos que conforman esta honorable institución. Por ello es que hemos creído conveniente efectuar el proyecto de tesis titulado “DISEÑO Y CONSTRUCCIÓN DE UN SISTEMA AUTOMATIZADO PARA LA GESTIÓN DE DOCUMENTOS EN LA ILUSTRE MUNICIPALIDAD DEL CANTÓN CALVAS UTILIZANDO CERTIFICADOS DIGITALES”, el cual está enmarcado en permitir enviar y recibir información de manera rápida, fácil, económica y segura. Los certificados digitales representan el punto más importante en tal acción ya que brindan una forma conveniente y fácil de

asegurar que los participantes en una transacción puedan confiar el uno en el otro. Esta confianza se establece a través de un tercero llamado Autoridad Certificadora, la cual se encarga de emitir certificados digitales.

En nuestro caso, hemos definido que el Municipio de Calvas actúe como Autoridad Certificadora, es decir se encargará de generar certificados digitales, mismos que serán solamente de uso interno; debido a que en la actualidad dicha institución no se encuentra registrada como una Autoridad Certificadora debidamente legalizada. En nuestro país el Banco Central del Ecuador es el único que está acreditado por el Consejo Nacional de Telecomunicaciones (CONATEL) mediante resolución Nª 481-20-2008 el 8 de Octubre del 2008, para encargarse de otorgar el título de Autoridad Certificadora a las instituciones públicas y privadas que requieran este vínculo de seguridad.

En este contexto, cada certificado digital, generará un par de claves denominadas públicas y privadas respectivamente. La clave pública será conocida por el resto de usuarios que intervengan en el proceso de envío y recepción de información, mientras que la clave privada será conocida únicamente por su propietario.

El proceso de generación de claves se logrará con la ayuda del algoritmo de encriptación asimétrica: RSA caracterizado porque cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada. Para comprobar que la información que se recibió es auténtica se utilizó el algoritmo MD5, el cual parte de la obtención de una cadena de 32 bits en formato hexadecimal, dicha cadena es la que se conoce como resumen o hash del mensaje que se recibió o envió, el cual más tarde permitirá verificar o refutar la firma digital del documento que fue enviado a través de la comparación de dichos hash obtenidos; uno que ya llegó con el documento recibido y el otro que se generó al momento de recibir o leer la información.

Todo este proceso requirió del uso de algunas herramientas de software: Windows Xp/ Vista como sistemas operativos. Netbeans, como herramienta de desarrollo de la aplicación.

JSF, como tecnología web, misma que se caracteriza principalmente por disponer de una arquitectura apropiada para manejar el estado de los componentes, procesar los datos, validar la entrada del usuario, y manejar eventos.

ICEFaces, encargado de crear componentes web de la interfaz JSF. ICEFaces permite utilizar técnicas Ajax de forma transparente, con un esfuerzo mínimo en Java/JSF.

Apache Tomcat, como servidor de la aplicación basada en entorno web. Tomcat puede funcionar como servidor web por sí mismo, es usado como servidor web autónomo en entornos con alto nivel de tráfico y alta disponibilidad. Dado que Tomcat fué escrito en Java, funciona en cualquier sistema operativo que disponga de la máquina virtual Java.

MYSQL como gestor de Base de Datos. Mysql es una base de datos muy rápida, segura y fácil de usar, además es multiusuario, multiplataforma y de código abierto.

Hibernate, el cual facilitó el mapeo de atributos entre la base de datos y el modelo de objetos de la aplicación

IReport, como diseñador de reportes. IReport es un constructor / diseñador de informes visual, poderoso, intuitivo y fácil de usar para JasperReports escrito en Java.

En lo que se refiere a la arquitectura de la aplicación utilizamos; la conocida como Modelo Vista Controlador, utilizada principalmente en el desarrollo de aplicaciones web, sus características principales son que el Modelo, las Vistas y los Controladores se tratan como entidades separadas; esto hace que cualquier cambio producido en el Modelo se refleje automáticamente en cada una de las Vistas.

Por otro lado es importante mencionar que se configuró la aplicación para que utilice el protocolo de seguridad https, con el fin de garantizar la seguridad de las comunicaciones entre el usuario y el servidor web al que éste se conecta.

Se espera en lo posterior que este sistema pueda ser implementado y mejorado, ya que así se logrará simplificar los procesos de gestión de la información y mejorar la fiabilidad y la velocidad con que se tratan los documentos, con el consiguiente incremento de eficacia, obtención de importantes ahorros y mayores beneficios para la institución.

5. METODOLOGÍA

La investigación es un factor muy importante que está destinado a realizar actividades intelectuales y experimentales de modo sistemático con el propósito de aumentar los conocimientos sobre un determinado hecho; razón por la cual facilita el descubrimiento de diferentes tipos de problemas que afectan a nuestro entorno, los cuales una vez que han sido detectados pueden ser analizados y posteriormente solucionados con algunas de las alternativas encontradas.

Para llevar a cabo este proceso fue necesario seguir un esquema metodológico, basado en el uso de métodos y técnicas encargadas de facilitar la recolección de datos y de guiar correctamente la presente investigación.

5.1. MÉTODOS

- **Método En foque de Sistemas**

Es un esquema metodológico que sirve como guía para la solución de problemas, en especial hacia aquellos que surgen en la dirección o administración de una institución. En nuestro caso el Municipio de Calvas presenta inconvenientes en lo referente a la administración documental, motivo por el cual resulta conveniente el desarrollar una aplicación encargada del flujo y seguridad (encriptación de datos) de dicha información. El enfoque de sistemas se basa en el uso de los métodos Deductivo e Inductivo así:

Deductivo

El cual se caracteriza principalmente por partir de datos generales aceptados como válidos para llegar a una conclusión de tipo particular. En nuestro caso para la construcción del Sistema Automatizado de Gestión de Documentos utilizando certificados digitales, se utilizó este método, ya que nos permitió determinar cuáles son los inconvenientes que se suscitan actualmente al momento de tramitar información de una oficina a otra en el Municipio de Calvas, es decir durante el envió y recepción de datos, denotando que la resolución de éste tipo de tareas es un proceso tedioso y que requiere que sea controlado debidamente en base a los estándares de seguridad y confidencialidad de información actualmente existentes. En el caso de esta institución dichas normas de seguridad están enmarcadas a través de la definición de contraseñas para cada usuario, de tal manera que no todos tengan acceso a la

información archivada; el Analista de Sistemas es el encargado de controlar la administración de tales datos.

Inductivo.

Se fundamenta en partir de los datos particulares para llegar a conclusiones generales. Para ello se utilizó una encuesta dirigida a miembros del Municipio de Calvas con la finalidad de determinar datos en lo referente a Gestión Documental existente en esta institución, luego de lo cual se efectuó un análisis que permitió determinar las causas que generan dichos inconvenientes y los efectos que éstos producen en el cumplimiento normal de actividades.

☞ **Método analítico – crítico**

Este método fué utilizado puesto que analizamos y sintetizamos los conocimientos, mismos que se basaron en la sustentación de la bibliografía, para luego ser plasmados en los resultados del proyecto.

☞ **Método Descriptivo**

Este método se utilizó en el momento en que se describió las características de la aplicación, conjuntamente con sus interfaces gráficas, además se realizó la explicación de cada función y procedimiento que se utilizó para la realización de la aplicación y por ende el cumplimiento del objetivo general en que se basa el presente proyecto de tesis.

☞ **Ciclo de Vida Clásico para el Desarrollo de Software**

Mediante el cumplimiento de etapas ordenadas, nos permitió obtener un producto fundamentado principalmente en las necesidades que existen y se verifican actualmente en el Ilustre Municipalidad del cantón Calvas. Las fases que se definieron dentro de ésta metodología fueron:

1. ***Análisis y determinación de los requerimientos del sistema*.-** En esta etapa se recolectó la información referente a los procesos que se efectúan al momento de tramitar algún tipo de documento considerando para ello el nivel de relación o vinculación entre una oficina dependencia y otra, siendo por tanto necesario el uso de algunas técnicas de recolección de datos tales como entrevistas y observación directa, con la finalidad de identificar las características que tendrá el nuevo sistema, incluyendo la información que el

sistema debe producir y las características operativas, como son controles de procesamiento, tiempos de respuesta y métodos de entrada y salida.

2. ***Diseño de la aplicación.-*** En esta fase se definió los detalles de la forma en que el sistema cumplirá con los requerimientos identificados durante la fase de análisis. Para ello se hizo uso de algunas de las herramientas automatizadas disponibles para el diseño de sistemas como la metodología ICONIX la cual se encargó de guiar la construcción de un prototipo que más tarde permitió la culminación del sistema, así como también nos permitió determinar los procedimientos a seguir para los datos de entrada, almacenamiento y salida del mencionado sistema.

3. ***Desarrollo del sistema.-*** Etapa en la cual desarrollamos los diferentes módulos que conformarán el sistema y que fueron especificados en la etapa anterior. Para ello fué necesario utilizar las herramientas de desarrollo como son: Windows Xp/ Vista como sistemas operativos, Apache Tomcat, como servidor de la aplicación, MYSQL como gestor de Base de Datos, JSF como entorno de programación Java, y Jasper Report encargado de la generación de reportes. En esta etapa también se creó toda la documentación necesaria para explicar, probar el programa y hacer el mantenimiento.

4. ***Pruebas y corrección.-*** Durante todo el desarrollo del software se realizaron pruebas de acuerdo a su funcionalidad específica, es decir se trabajó por módulos; ello con la finalidad de lograr corregir errores desde el inicio. Así mismo el sistema se empleó de manera experimental para asegurarnos que no tenga fallas, y funcione de acuerdo con las especificaciones y en la forma en que los usuarios esperan que lo haga. Se empleó datos reales para dichas pruebas y después se procedió a examinar los resultados.

☞ **Metodología para el desarrollo de la aplicación**

ICONIX, Basada principalmente en la adopción de casos de uso, está definida como un Proceso de Desenvolvimiento desarrollado para Ingeniería de Software. Por ello es de que su enfoque fué el siguiente:

- ✓ Modelado de objetos conducido por casos de uso

- ✓ Basado en escenarios que descomponen los casos de uso
- ✓ Enfoque iterativo e incremental
- ✓ Trazabilidad
- ✓ Uso directo de UML.

Los pasos que se siguieron para aplicar ésta metodología fueron los siguientes:

- ✓ Análisis de requerimientos: Luego de efectuar algunas entrevistas al personal del Municipio de Calvas, se detectó que existen algunos inconvenientes al momento de tramitar documentos entre las oficinas de esta institución, así como también falta de organización y almacenamiento de los datos además de no existir seguridades necesarias en lo que a información se refiere. En vista de aquello en esta etapa se cumplió con las siguientes tareas:
  - Identificar objetos del dominio y relaciones de agregación y generalización.
  - Determinación de requerimientos funcionales y no funcionales

- ✓ Análisis y diseño preliminar: Luego de haber establecido los requerimientos de la aplicación se procedió a realizar el diseño preliminar, el cual tuvo como finalidad él:

  - Prototipo rápido.- Basado principalmente en la definición de funciones específicas de la aplicación como administración de usuarios, categorías a las que cada documento pertenecerá y gestión de documentos para permitir el envío y recepción de información.
  - Identificar casos de uso.
  - Escribir descripciones de casos de uso (Cursos normales y alternos)

- ✓ Diseño: Etapa en la cual realizamos una revisión crítica del diseño inicial, y a la vez cumplimos con:

  - Modelado de casos de uso
  - Realizar diagramas de clases.
  - Definir el modelo conceptual y físico de la base de datos.
  - Realizar diagrama de paquetes.
  - Realizar diagrama de componentes.
  - Realizar diagrama de despliegue
  - Elaboración de diagramas de robustez.

- Elaboración de diagramas de secuencia
- Verificar cumplimiento de requerimientos.

✓ Pruebas e Implantación: Etapa en la cual efectuamos las pruebas necesarias en el sistema, orientadas al cumplimiento de los requerimientos definidos en la etapa de análisis. Las pruebas estuvieron orientadas a funcionalidad, aceptación y usabilidad. Por su parte la implantación consistió en una prueba piloto que se desarrolló en las instalaciones del Municipio de Calvas.

5.2. TÉCNICAS APLICADAS

☞ **Entrevista,** que fué realizada a los encargados de cada oficina del Municipio de Calvas (Ver Anexo 3), con la finalidad de obtener la información necesaria acerca del funcionamiento de los diferentes procesos que se efectúan al momento de tramitar algún tipo de documento ya sea durante su envió como en su recepción.

☞ **Lectura Científica,** misma que la utilizamos para investigar todos los referentes teóricos sobre seguridad, confidencialidad, certificados digitales y demás temas que nos facilitaron la sustentación del presente proyecto de tesis.

6. FUNDAMENTACIÓN TEÓRICA

CAPITULO I: GESTIÓN DOCUMENTAL

1.1. Definición

1.2. Aspectos de la Gestión Documental

1.3. Componentes de la gestión documental

1.4. Flujo de un Sistema de Gestión Documental

- **1.4.1.** Elementos

1.5. Ventajas y desventajas

CAPITULO II: CERTIFICADOS DIGITALES

2.1. Definición

2.2. Formato de un certificado digital

2.3. Tipos de Certificados Digitales

2.4. Emisores de certificados

- **2.4.1.** Autoridades de Certificación
- **2.4.2.** Jerarquía de Autoridades Certificantes

2.5. Firma Digital

- **2.5.1.** Definición
- **2.5.2.** Funciones hash
  - **2.5.2.1.** Algoritmo MD5
- **2.5.3.** Proceso de Firma y Verificación de Firma
- **2.5.4.** Tipos
- **2.5.5.** Claves Privadas y Públicas
- **2.5.6.** Criptografía
  - **2.5.6.1.** Definición
  - **2.5.6.2.** Tipos de Criptografía
  - **2.5.6.3.** Algoritmo de Encriptación RSA

CAPITULO III: SEGURIDAD

3.1. Definiciones Básicas.

- **3.1.1.** Confidencialidad.
- **3.1.2.** Integridad.
- **3.1.3.** Disponibilidad.
- **3.1.4.** Conceptos relacionados

CAPITULO IV: AUDITORIA INFORMÁTICA

CAPITULO V: TECNOLOGÍAS PARA EL DESARROLLO DE LA APLICACIONES WEB

CAPITULO VI: ILUSTRE MUNICIPIO DE CALVAS

6.1. Historia.

6.2. Base Legal

6.3. Misión

6.4. Visión

6.5. Objetivos Estratégicos

6.6. Objetivos Operativos

6.7. Estructura Programática

6.8. Servicios Generales

- **6.8.1.** Administración General
- **6.8.2.** Administración Financiera
- **6.8.3.** Justicia, Policía y Vigilancia

6.9. Servicios Comunales

- **6.9.1.** Planificación Urbana y Rural
- **6.9.2.** Higiene Ambiental: Unidad de Medio Ambiente y Turismo

6.10. Otros servicios comunales

6.11. Servicios Económicos

- **6.11.1.** Transporte y vías

6.12. Servicios Inclasificados

CAPITULO I: GESTIÓN DOCUMENTAL

1.1. Definición

Se entiende por gestión documental al conjunto de normas técnicas y prácticas usadas para administrar el flujo de documentos de todo tipo en una organización, permitir la recuperación de información desde ellos, determinar el tiempo que los documentos deben guardarse, eliminar los que ya no sirven y asegurar la conservación indefinida de los documentos más valiosos, aplicando principios de racionalización y economía.

No obstante, las tecnologías de la información han permitido hacer grandes avances en la gestión documental, mediante los Sistemas de Gestión Documental (DMS, del inglés, Document Management System)[1]. Estos sistemas permiten informatizar la gestión, haciendo los procesos más ágiles, más eficientes, y con un ahorro sustancial de espacio físico.

1.2. Aspectos de la Gestión Documental

La gestión documental puede abarcar muchos grados de complejidad, dependiendo de la cantidad de documentación que haya, y el grado de eficiencia con el que se quiera gestionar. No obstante, existen unos aspectos básicos, o unos criterios que hay que tener en cuenta para gestionar documentos, y cuando se implanta un sistema de gestión documental. En la tabla 1 se muestran algunos aspectos:

Criterios	
Localización	Dónde se almacenarán los documentos. Cómo se accederá a ellos
Clasificación	Cómo se organizarán. Qué métodos se usarán para guardarlos de manera que luego sean fácilmente recuperables.
Recuperación	Cómo se encuentran los documentos. Existencia de algún tipo de buscador. Relacionado con la clasificación
Seguridad	Políticas de seguridad que definan cómo proteger los documentos de personal no autorizado, y los distintos niveles de autorización
Recuperación de desastres	Políticas de protección contra desastres, y recuperación de la información en caso de que estos sucedan.

[1] La gestión documental se considera como parte del área más amplia de ECM ("Enterprise Content Management" o "Gestión de contenido empresarial").

Custodia	Qué documentos conservar y durante cuánto tiempo. Qué documentos se pueden eliminar.
Distribución	Cómo se distribuyen los documentos para quienes los necesitan. Qué sistema de distribución se elige.
Workflow	Flujo entre las diferentes personas de la organización. Establecimiento de reglas para que este flujo sea ágil, seguro y cumpla las normas de seguridad de los documentos.
Creación	Cómo se crean documentos en un entorno colaborativo, controlando las versiones y niveles de autorización
Autenticación	Validación de la autenticidad de los documentos.

Tabla 1. Aspectos de la Gestión Documental

1.3. Componentes de la gestión documental

Los sistemas informáticos de gestión documental suelen integrar una serie de elementos comunes a todos ellos, tales como:

Metadatos

Al margen de la información contenida en el documento, conviene almacenar información del propio documento: fecha de creación, autor, tamaño, propiedades, compañía, materia que trata, entre otros. Actualmente prácticamente cualquier aplicación informática que genere documentos es capaz de almacenar todos estos metadatos.

Integración

Integración de todo tipo de documentos en la misma aplicación de gestión de forma que un usuario pueda crearlo, abrirlo, editarlo, guardar nueva versión, todo sin salir de la aplicación.

Captura

Posibilidad de obtener y digitalizar documentos como imágenes, o textos que se tienen en papel u otros formatos, escaneándolos. Esto incluye funcionalidad OCR, (reconocimiento de texto), que al escanear texto lo traslada a documento de texto, en vez de documento de imagen. Una vez digitalizados es posible integrarlos en el sistema de gestión informático.

Indexación

Consiste en poner identificadores únicos a los documentos de forma que sean más sencillos de localizar. Además de esto, cuando el volumen de documentos es grande conviene utilizar otras técnicas como categorización y agrupaciones de índices para que se puedan hacer búsquedas en árbol y no sea necesario recorrer todos los elementos en una búsqueda.

Almacenamiento

Almacenamiento de los documentos electrónicos, en una base de datos. Contemplará funcionalidad para definir cuánto tiempo se mantienen, cómo hacer migraciones a otro sistema de almacenamiento, copias de seguridad, recuperación en caso de fallo, etc.

Recuperación

Herramientas para recuperar un determinado archivo almacenado. No siempre se conocerá el identificador único del archivo, por lo que la aplicación debería proporcionar la posibilidad de encontrarlo por título, u otros metadatos como tamaño, autor, etc, pudiendo hacer búsquedas más eficientes.

Distribución

La aplicación deberá proporcionar un canal de distribución de los archivos, en caso de que estos deban ser distribuidos.

Seguridad

La aplicación debe garantizar que los documentos tengan el nivel de seguridad adecuado. Habrá documentos con información sensible que no deberían poder ser accedidos más que por el personal indicado. Además, debe aportar seguridad frente a posibles intrusiones externas a la organización. La seguridad está determinada principalmente por la definición de roles: administrador y usuario; así como también por password o contraseñas.

Workflow

El flujo de transmisión de los documentos se define por parte de la organización, por ejemplo: un empleado crea un documento técnico, un supervisor debe aprobarlo, y

después alguien de administrador debe firmarlo, es decir la aplicación debe ser capaz de manejar los flujos definidos por la organización y seguirlos de forma automática.

Control de versiones

Como muchas personas pueden trabajar sobre el mismo documento, es necesario llevar un control de versiones del mismo. Las aplicaciones de gestión documental suelen integrar esto, de forma que cada vez que un documento se modifica se guarda un histórico con el autor y los cambios realizados.

1.4. Flujo de un Sistema de Gestión Documental

1.4.1. Elementos

Bases de Datos

La aplicación de la informática en todos los niveles de las organizaciones comprende un fenómeno que tiene sus implicaciones en la gestión documental: la proliferación de bases de datos sobre distintos aspectos, que en algunos casos están sustituyendo a los documentos como soporte de información valiosa para la organización.

Desde un punto de vista de gestión documental, uno de los principales problemas es cómo identificar los documentos dentro del entorno de la BD, saber qué parte del contenido constituye los documentos que se han de gestionar.

Hardware

Escáneres y dispositivos de Digitalización: Los documentos originales, una vez preparados, son transformados en documentos digitales, los cuales serán guardados o almacenados.

Servidores: Contienen la información previamente almacenada. Los usuarios finales se conectaran a un servidor para poder acceder a dicha información[2].

Software

Gestores documentales: Programas de apoyo al proceso de gestión de la documentación que se maneja en la empresa.

[2] Wikipedia, (2010) Flujo del Sistema de Gestión Documental [en línea] Disponible en: http://es.wikipedia.org/wiki/Gestión_documental

Redes

Por medio de la red los usuarios podrán acceder a la información que se encuentra en los servidores de un determinado sistema. La red pueden ser local, aunque también se puede acceder a la información por Internet.

Usuarios

A través de una cuenta de Usuario, se lleva a cabo el acceso a los documentos digitalizados dentro del Sistema de Gestión Documental permitiendo así, realizar la consulta electrónica de los mismos de acuerdo a los niveles de seguridad asignados a cada uno de los usuarios registrados en el Sistema.

1.5. Ventajas y desventajas

Implantar un sistema de gestión documental tiene las siguientes ventajas y desventajas:

Ventajas

- **Sencillez y accesibilidad**: de una forma sencilla y rápida se tiene acceso a toda la documentación de la empresa.
- **Seguridad**: la información se encuentra más segura contra pérdidas, y contra accesos no autorizados.
- **Ahorro**: reducción del espacio de almacenamiento, y del tiempo empleado en hacer búsquedas y en almacenar información.
- **Uso compartido**: La documentación es accesible por todos y como recurso colectivo. Esto evita duplicaciones, gastos en copias, etc.
- **Productividad mejorada**: la productividad mejora al tener un acceso más eficiente y rápido a la información.

Desventajas

- **Costo de implantación**: Implantar uno de estos sistemas puede suponer un alto costo económico.
- **Tiempo de implantación**: si el volumen de datos a introducir en el sistema la primera vez es muy grande, puede llevar mucho tiempo y recursos esta digitalización

CAPITULO II: CERTIFICADOS DIGITALES

2.1. Definición

Un certificado digital es un mecanismo informático por medio del cual se garantiza técnicamente la identidad de una persona u entidad, así como también la autenticidad e integridad de un documento.

Los certificados digitales tienen una duración determinada, transcurrida la cual deben ser renovados, y pueden ser revocados anticipadamente en ciertos supuestos (por ejemplo, en el caso de que la clave privada, haya pasado a ser conocida por personas no autorizadas, pérdida del dispositivo de almacenamiento, ausentismo prolongado de su propietario por motivo de viaje, o fallecimiento inesperado).

Gracias a un certificado digital, podemos estar seguros de la identidad de una persona, proceso que se basa en el uso de un par de claves; una pública y una privada. Por lo tanto si sabemos que el mensaje ha sido cifrado con la clave privada de esa persona, sabremos también quien es la persona titular de esa clave.

Si bien existen variados formatos para certificados digitales, los más comúnmente empleados se rigen por el estándar UIT-T X.509[3]. El certificado contiene usualmente el nombre de la entidad certificada, número de serie, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su firma digital) y la firma digital de la autoridad emisora del certificado de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación.

En lo que se refiere a la validez de un Certificado Digital, tendrá validez por el lapso de 2 años a partir de la fecha de emisión, expirada dicha fecha podrá renovarse 2 veces como máximo, por lapsos similares.

La solicitud de renovación deberá efectuarse, en todos los casos, antes del vencimiento del plazo de validez original del certificado o del de la primera renovación, según corresponda.

[3] Estándar para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI). La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, y otros usos.

2.2. Formato de un certificado digital

Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

- Nombre, dirección y domicilio del suscriptor.
- Identificación del suscriptor nombrado en el certificado.
- El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
- La clave pública del usuario.
- La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
- El número de serie del certificado.
- Fecha de emisión y expiración del certificado.

Formato de un certificado digital X.509

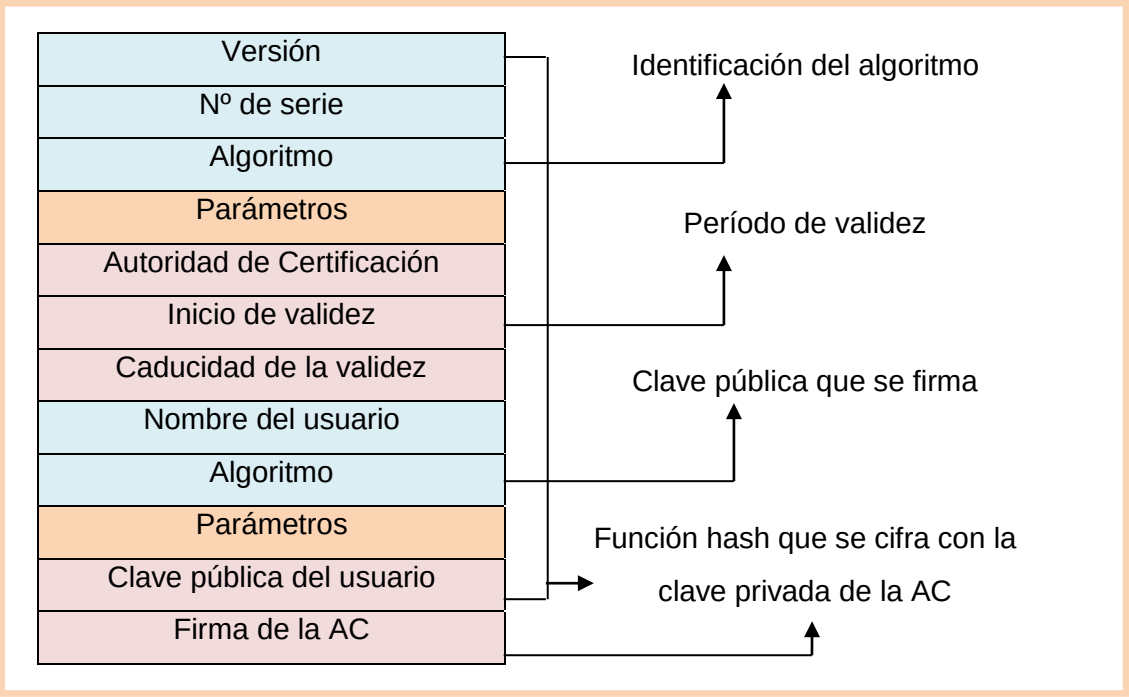


Fig. 1. Formato de un certificado digital X509

Campos del certificado digital X.509

- V: Versión del certificado (actualmente V3).
- SN: Número de serie.

- AI: identificador del algoritmo de firma que sirve para identificar el algoritmo usado para firmar el paquete X.509.
- CA: Autoridad certificadora.
- T_A: Periodo de validez.
- A: Propietario de la clave pública que se está firmando.
- P: Clave pública más identificador de algoritmo utilizado y más parámetros si son necesarios.
- Y{I}:Firma digital de Y por I usando la clave privada de la unidad certificadora.

2.3. Tipos de Certificados Digitales

Las Autoridades de Certificación pueden emitir diferentes tipos de certificados; básicamente son: Certificados de Identidad (personal o digital), Certificados de Autorización (potestad), Certificados Transaccionales (actas y resguardos), y Certificados de Tiempo (estampillado o registro temporal).

- Los Certificados de Identidad son los más utilizados actualmente dentro de los criptosistemas de clave pública[4] y ligan una identidad personal (usuario) o digital (equipo, software, etc.) a una clave pública.

- Los Certificados de Autorización o potestad son aquellos que certifican otro tipo de atributos del usuario distintos a la identidad, como pueden ser, el pertenecer a una determinada asociación, disfrutar de una serie de privilegios, poseer un carnet de conducir, etc.

- Los Certificados Transaccionales son aquellos que atestiguan que algún hecho o formalidad acaeció o fue presenciada por un tercero; el agente de registro al servicio de la Autoridad de Certificación emisora.

- Los Certificados de Tiempo o de estampillado digital de tiempo permiten dar fe de que un documento existía en un instante determinado de tiempo, por lo que constituyen un elemento fundamental de todos los servicios de registro documental y de protección de la propiedad intelectual o industrial que se están proponiendo.

[4] En los criptosistemas de clave pública, la clave de cifrado se hace de conocimiento general (se le llama clave pública). Sin embargo, no ocurre lo mismo con la clave de descifrado (clave privada), que se ha de mantener en secreto. La existencia de ambas claves diferentes, para cifrar o descifrar, hace que también se conozca a estos criptosistemas como asimétricos.

2.4. Emisores de certificados

Cualquier individuo o institución puede generar un certificado digital, pero si éste emisor no es reconocido por quienes interactúen con el propietario del certificado, el valor del mismo es prácticamente nulo. Por ello los emisores deben acreditarse: así se denomina al proceso por el cual entidades reconocidas, generalmente públicas, otorgan validez a la institución certificadora, de forma que su firma pueda ser reconocida como fiable, transmitiendo esa fiabilidad a los certificados emitidos por la citada institución.

Pero para que un certificado digital tenga validez legal, el prestador de Servicios de Certificación debe acreditarse en cada país de acuerdo a la normativa que cada uno defina. Encargados de autorizar la creación de una autoridad de certificación o prestador de servicios de certificación de algunos países hispanos son:

- En Chile, el Ministerio de Economía;
- En Colombia, la Sociedad Cameral de Certificación Digital Certicámara y Gestión de Seguridad Electronica;
- En Ecuador, el Banco Central del Ecuador;
- En España: la Fábrica Nacional de Moneda y Timbre, el Ministerio de Industria, Turismo y Comercio, la Agencia Catalana de Certificación, etc;
- En Guatemala, el Ministerio de Economía;
- En México, la Secretaría de Economía;
- En Perú, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual;
- En la República Dominicana el Instituto Dominicano de las Telecomunicaciones;
- En Venezuela, la Superintendencia de Servicios de Certificación Electrónica.

2.4.1. Autoridades de Certificación

La validez de un certificado es la confianza en que la clave pública contenida en el certificado pertenece al usuario indicado en el certificado. La manera en que se puede confiar en el certificado de un usuario con el que no hemos tenido una vinculación anterior es mediante la confianza en terceras partes.

La idea consiste en que dos usuarios puedan confiar entre sí, si ambos tienen relación con una tercera parte la cual podrá dar fé de la fiabilidad de los dos, la cual la constituye la Autoridad Certificante.

Una Autoridad Certificante es una tercera parte en la cual otros confían y que se encarga de establecer la vinculación entre una clave pública y su propietario[5].

La necesidad de una tercera parte de confianza es fundamental en cualquier entorno de clave pública de tamaño considerable debido a que es improbable que los usuarios hayan tenido relaciones previas antes de intercambiar información cifrada o firmada.

Por otra parte, la mejor manera de permitir la distribución de las claves públicas (o certificados digitales) de los distintos usuarios es que algún agente en quien todos los usuarios confíen se encargue de su publicación en algún repositorio al que todos los usuarios tengan acceso.

La forma en que esta tercera parte avalará que el certificado de un determinado usuario es válido será mediante su firma digital sobre dicho certificado.

2.4.2. Jerarquía de Autoridades Certificantes

Las CA disponen de sus propios certificados públicos, cuyas claves privadas asociadas son empleadas por las CA para firmar los certificados que emiten. Un certificado de CA puede estar auto-firmado cuando no hay ninguna CA de rango superior que lo firme. Este es el caso de los certificados de CA raíz, el elemento inicial de cualquier jerarquía de certificación. Una jerarquía de certificación consiste en una estructura jerárquica de CAs en la que se parte de una CA auto-firmada, y en cada nivel, existe una o más CAs que pueden firmar certificados de entidad final (titular de certificado: servidor web, persona, aplicación de software) o bien certificados de otras CA subordinadas plenamente identificadas y cuya Política de Certificación sea compatible con las CAs de rango superior.

Por lo tanto es de notar que este proceso podría seguirse indefinidamente y no tendría fin, el problema no se resolvería. Se hace necesario entonces cortar la cadena en algún punto de manera tal que habrá una autoridad certificante de nivel superior a todas las demás, llamada autoridad certificante raíz, dicho proceso se indica en la fig. N° 2

[5] Cámara de Gipuzcoa, (2005) Certificación Digital [en línea] Disponible en: http://www.camaragipuzkoa.com/certificaciondigital/informacion_general/CAs.php

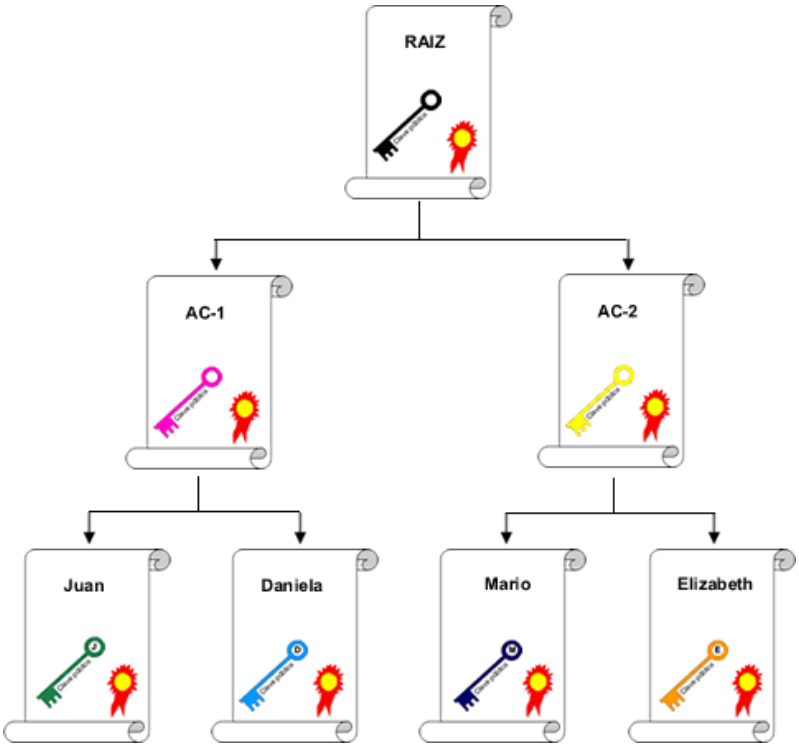


Fig. 2. Jerarquía de autoridades certificadoras

2.5. Firma Digital

2.5.1. Definición

La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos gocen de una característica que únicamente era propia de los documentos en papel.

Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje.

La firma digital es un instrumento con características técnicas y normativas. Esto significa que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen.

Las firmas digitales deben tener las mismas propiedades que las escritas:

- Únicas. Una firma digital debe de ser generada únicamente por su usuario.
- No se podrán falsificar. La generación por parte de otros usuarios de firmas de cara a falsificar una firma digital será imposible, es decir tendrán que resolver

problemas intratables de una gran complejidad mientras intentan falsificas la firma.

2.5.2. Funciones hash

La firma digital de un documento no es un passwords, es el resultado de aplicar cierto algoritmo matemático, denominado función hash, al contenido.

Esta función asocia un valor dentro de un conjunto finito (generalmente los números naturales) a su entrada. Cuando la entrada es un documento, el resultado de la función es un número que identifica casi unívocamente al texto.

Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido.

Para poder realizar una firma digital, es necesario primero convertir el mensaje en un número. Este número es entregado a la función hash, que produce el resumen del mensaje. Esta función convierte un número grande (el mensaje) en un número pequeño (el resumen).

El número pequeño del resumen suele tener una longitud de 128 bits (MD5), o de 160 bits (SHA-1). Cada BIT puede ser tanto un "0" como un "1". El proceso de obtención del resumen a partir del mensaje debe ser determinístico[6]. Debe ser repetible. El mismo mensaje siempre debe dar el mismo resumen. Si no, el proceso de verificación no funcionaría.

Para que una función de hash sea buena, debe ser una función unidireccional. Debe funcionar en un sentido, pero no en el contrario. Además debe ser muy difícil encontrar dos mensajes diferentes que produzcan el mismo resumen.

2.5.2.1. Algoritmo MD5

El algoritmo MD5 es una función de cifrado tipo hash que acepta una cadena de texto como entrada, y devuelve un número de 128 bits o cadena de 32 caracteres en notación hexadecimal. Las ventajas de este tipo de algoritmos son la imposibilidad (computacional) de reconstruir la cadena original a partir del resultado, y también la imposibilidad de encontrar dos cadenas de texto que generen el mismo resultado.

[6] Un valor determinístico es aquel en que se obtiene siempre el mismo resultado bajo las mismas condiciones iniciales.

Esto nos permite usar el algoritmo para transmitir contraseñas a través de un medio inseguro. Simplemente se cifra la contraseña, y se envía de forma cifrada. En el punto de destino, para comprobar si el password es correcto, se cifra de la misma manera y se comparan las formas cifradas.

Ejemplos de MD5:

Mensaje	Hash generado
hola	4d186321c1a7f0f354b297e8914ab240
La casa de la pradera en lo alto del río	92346a0999803dd9d63184e9c4749e11
La casa de la pradera en lo alto de la ría	cfb04578d958bac2288ca2cdecaf13c5

Tabla 2. Ejemplo de generación de hash

Como se aprecia en los hashes anteriores, el resultado generado tiene una longitud fija, independiente del tamaño del mensaje de entrada.

El hash MD5 es constante para cada cadena. Es decir: el hash de "hola" es **SIEMPRE** "4d186321c1a7f0f354b297e8914ab240". Vemos también como, a pesar de lo similares que son los dos últimos mensajes, su resultado es radicalmente distinto. Esto es una característica muy importante del algoritmo MD5 puesto que, errores o variaciones muy pequeñas en la entrada provocan enormes diferencias en la salida.

Cuando se producen errores en la transmisión, un solo bit erróneo dentro de un archivo de muchos megabytes puede ser fatal. En caso de existir esa pequeña variación entre el archivo original y el recibido, nos daremos cuenta por lo diferente de su hash MD5.

El algoritmo MD5 estima que hallar dos hashes iguales para diferentes cadenas supone una dificultad de 2^{64} intentos (tendríamos que hallar 1.84467440737E+19 hashes diferentes para encontrarnos con uno de estos).

Por otro lado es importante indicar que un hash no se puede desencriptar porque es un algoritmo de un solo sentido. Hay que tomar en cuenta que si fuésemos capaces de desencriptar hashes MD5, habríamos inventado el algoritmo de compresión más potente del mundo. Por todo ello es que el algoritmo MD5 estima que, dado un hash cualquiera, la dificultad de encontrarse con el mensaje que lo produjo es de 2^{128} intentos (3.40282366921E+38, tarea computacionalmente imposible).

Funcionamiento y descripción del algoritmo md5

Empezamos suponiendo que tenemos un mensaje de 'b' bits de entrada, y que nos gustaría encontrar su resumen. Aquí 'b' es un valor arbitrario entero no negativo, pero puede ser cero, no tiene por qué ser múltiplo de ocho, y puede ser muy extenso. Imaginemos los bits del mensaje escritos así:

m0 m1……..m{b-1}

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

Paso 1. Adición de bits

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

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

Paso 2. Longitud del mensaje

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

En este punto el mensaje resultante (después de rellenar con los bits y con 'b') se tiene una longitud que es un múltiplo exacto de 512 bits. A su vez, la longitud del mensaje es múltiplo de 16 palabras (32 bits por palabra).

Con M[0 ... N-1] denotaremos las palabras del mensaje resultante, donde N es múltiplo de 16.

Paso 3. Inicializar el búfer MD

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

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

Paso 4. Procesado del mensaje en bloques de 16 palabras

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

- F(X,Y,Z) = (X ^ Y) V (¬ X ^ Z)
- G(X,Y,Z) = (X ^ Z) V (Y ^ ¬Z)
- H(X,Y,Z) = X ⊗ Y ⊗ Z
- I (X,Y,Z) = Y ⊗ (X V ¬Z)

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

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

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

Paso 5. Salida

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

2.5.3. Proceso de Firma y Verificación de Firma

En el siguiente ejemplo, se describe el proceso de la firma y verificación de firma, para el envío y recepción de un correo electrónico:

Recordemos que Juan y Mario tienen sus pares de claves correspondientes, como se observa en la Fig. 3.

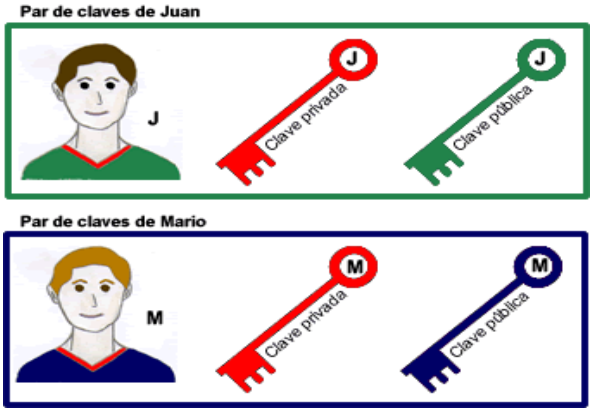


Fig. 3. Par de claves asignadas a las personas involucradas en la comunicación

Proceso de Firma

El proceso de firma es el siguiente:

- El usuario prepara el mensaje a enviar.
- El usuario utiliza una función hash segura para producir un resumen del mensaje.
- El remitente encripta el mensaje original con su clave privada. La clave privada es aplicada al texto usando un algoritmo matemático.
- El remitente envía electrónicamente el mensaje encriptado, y el hash generado.
- El destinatario usa la clave pública del remitente para verificar la firma digital, es decir para desencriptar el mensaje original.
- El destinatario realiza un resumen del mensaje desencriptado utilizando la misma función resumen segura.

- El destinatario compara los dos resúmenes. Si los dos son exactamente iguales el destinatario sabe que los datos no han sido alterados desde que fueron firmados.

Juan escribe un correo electrónico a Mario. Es necesario que Mario pueda verificar que es Juan quien ha enviado el correo. Por ello, Juan debe enviar el correo firmado digitalmente.

Cuando Juan le indica al programa de correo que envíe el mensaje firmado digitalmente, éste realizará las siguientes operaciones, detalladas en la Fig. 4.

- Procesa el mensaje mediante una función hash y obtiene la huella digital (número) o resumen.
- Cifra el resumen utilizando la clave privada que Juan ingresa. Como resultado se obtiene la firma digital del mensaje.
- Envía a Mario el mensaje original junto con la firma digital del mensaje y la correspondiente clave pública.

Verificación de Firma

Mario recibe el correo junto con la firma digital. Tiene que comprobar la validez de la misma para dar por bueno el mensaje y reconocer al autor (integridad y autenticación).

En el momento que Mario recibe el mensaje, el programa de correo electrónico realizará las siguientes operaciones, detalladas en la Fig. 4

- Descifra la firma digital con la clave pública recibida de parte de Juan y obtiene el número de hash (huella digital o resumen) original producido por Juan.
- Aplica al mensaje recibido la función hash para obtener una huella digital o resumen.
- Compara la huella digital recibida con la obtenida en el punto anterior. Si son iguales, Mario podrá estar seguro de que quien ha enviado el mensaje es Juan y que el mismo no ha sido modificado. Si son diferentes entonces significa que el mensaje ha sufrido alguna alteración posterior al envío.

Con este sistema conseguimos: Autenticación la firma digital es equivalente a la firma manuscrita de un documento, integridad: el mensaje no podrá ser modificado, no repudio en origen: el emisor no puede negar haber enviado el mensaje.

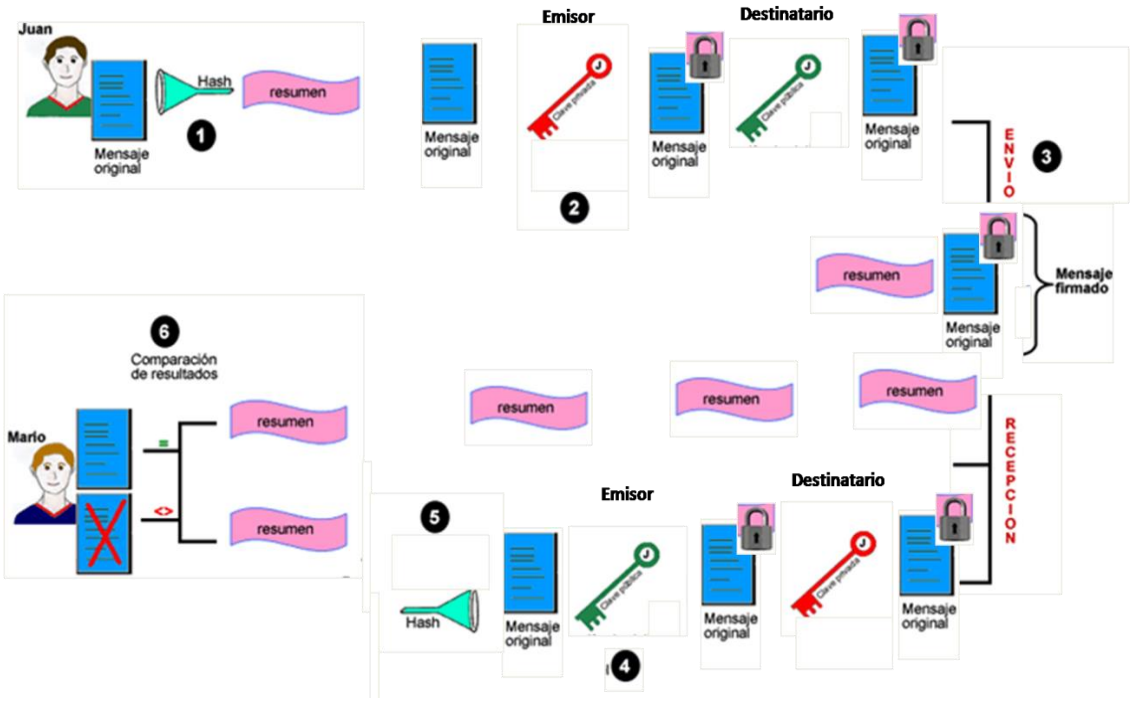


Fig. 4 Proceso de firma y verificación de firma

2.5.4. Tipos

Según la ley de firma digital, que puede ser diferente en cada país, define tres tipos de firma digital:

- Simple: incluye un método de identificar al firmante.
- Avanzada: además de identificar al firmante permite garantizar la integridad del documento. Se emplean técnicas de PKI, las cuales se basan en el uso de dispositivos de almacenamiento seguros para claves privadas conocidos generalmente como tokens o tarjetas criptográficas.
- Reconocida: es la firma avanzada ejecutada con un DSCF (dispositivo seguro de creación de firma) y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante).

2.5.5. Claves Privadas y Públicas

Cada titular de una firma digital posee un par de claves asociadas, una privada y otra pública, generada mediante un proceso matemático. Ambas claves se encuentran asociadas entre sí por las características especiales de dicho proceso matemático,

basado principalmente en la criptografía asimétrica (también llamada criptografía de clave pública).

A continuación en la tabla 3 se detalla la utilidad de cada clave:

Clave	Utilidad
CLAVE PRIVADA	Es utilizada por su titular para firmar digitalmente un documento o mensaje, es secreta y mantenida por ese titular bajo su exclusiva responsabilidad
CLAVE PUBLICA	Es utilizada por el receptor de un documento o mensaje firmado para verificar la integridad y la autenticidad, asegurando el "no repudio".

Tabla 3. Usos de las claves públicas y privadas

En un sistema criptográfico asimétrico, cada usuario posee un par de claves propio. Estas dos claves privada y pública, poseen la característica de que si bien están fuertemente relacionadas entre sí, no es posible calcular la primera a partir de los datos de la segunda.

El sistema opera de tal modo que la información cifrada con una de las claves sólo puede ser descifrada con la otra. De este modo si un usuario cifra determinada información con su clave privada, cualquier persona que conozca su clave pública podrá descifrar la misma.

En consecuencia, si es posible descifrar un mensaje utilizando la clave pública de una persona, entonces puede afirmarse que el mensaje lo generó esa persona utilizando su clave privada (probando su autoría).

2.5.6. Criptografía

2.5.6.1. Definición

Es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y es empleada frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que

el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito

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

2.5.6.2. Tipos de Criptografía

Criptografía Simétrica

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

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

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

Criptografía Asimétrica

La criptografía asimétrica es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso

a ella. 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.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del mismo podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje. Este proceso se puede dar también en sentido contrario, si se utiliza la clave privada, dicho mensaje solo podrá ser descifrado con la clave pública correspondiente, debido a que el par de claves son dependientes la una de la otra.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear.

2.5.6.3. Algoritmo de Encriptación RSA

El sistema criptográfico con clave pública RSA[7] es un algoritmo asimétrico cifrador de bloques, que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario. Una clave es un número de gran tamaño, que una persona puede conceptualizar como un mensaje digital, como un archivo binario o como una cadena de bits *o* bytes. Cuando se envía un mensaje, el emisor busca la clave pública de cifrado del receptor y una vez que dicho mensaje llega al receptor, éste se ocupa de descifrarlo usando su clave oculta. Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 00010100) elegidos al azar para conformar la clave de descifrado.

Funcionamiento

El algoritmo RSA, parte en primer lugar de la generación de los pares de claves pública (*e,n*) y privada (*d,n*)

- Elegimos dos números primos grandes *p* y *q* (entre más grandes es más segura la encriptación, pero es más demorado el proceso de

[7] RSA es una sigla formada por las iniciales del primer apellido de sus fundadores, Ron**R**ivest, Adi **S**hamir y Len Adleman, profesores del Massachusetts Institute of Technology.

encriptar/desencriptar) que sean diferentes y totalmente independientes el uno del otro. Calculamos *n=p*q*

- Se calcula fi: fi(n)=(p-1)(q-1)
- Se calcula e de manera que se cumpla que MCD(e, fi(n))=1 , y MCD (e, fi(n))=2
- Calculamos d=((Y*fi(n))+1)/e para Y=1,2,3,... hasta encontrar un d entero.
- El par de números (e,n) son la clave pública y el par de números (d,n) son la clave privada.

Encriptando datos

Para encriptar los datos el proceso consiste en consultar la clave pública del destinatario, dividir el mensaje que quiere enviar, asignarle un alfabeto numérico a cada fragmento y calcular para cada división: C = M^e mod n (M= mensaje original)

Desencriptando

Con el mensaje que le ha llegado al destinatario, lo que tiene que hacer es dividirlo y usar su clave privada para calcular: M = C^d mod n

Ejemplo: Los parámetros usados en el siguiente ejemplo son pequeños y orientativos con respecto a los que maneja el algoritmo, debido a que cuando se encripta algún tipo de texto generalmente es extenso.

Valor	Significado
p=3	1º nº primo Privado
q=11	2º nº primo Privado
n=pq=33	producto p*q
e=3	exponente Público
d= 7	exponente Privado

Tabla 4. Ejemplo de generación de claves con RSA

La clave pública (e, n). La clave privada es d. La función de cifrado es:

$$\mathbf{C = M^e \bmod n \Rightarrow} \; C = 5^3 \bmod (33) = 26$$

Donde m es el texto sin cifrar. La función de descifrado es:

$$\mathbf{M = C^d \bmod n \Rightarrow} \; M = 26^7 \bmod 33 = 8031810176 \bmod 33 = 5$$

Ambos de estos cálculos pueden ser eficientemente usados por el algoritmo de multiplicación cuadrática para exponenciación modular.

CAPITULO III: SEGURIDAD

3.1. Definiciones Básicas.

3.1.1. Confidencialidad.

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados[8].

Es por ello que las medidas de seguridad deben estar enfocadas a garantizar que la información está disponible para aquellos que estén autorizados a conocerla. Es crítica cuando los datos proporcionan ventaja competitiva en fabricación o confianza del consumidor.

3.1.2. Integridad.

Para la seguridad de la Información, la integridad es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información.

3.1.3. Disponibilidad.

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizada para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente.

3.1.4. Conceptos relacionados

- **Auditabilidad.-** Permitir la reconstrucción, revisión y análisis de la secuencia de eventos

[8] Wikipedia, (2010) Seguridad de la información [en línea] Disponible en: http://es.wikipedia.org/wiki/Seguridad_de_la_información

- **Identificación.-** Verificación de una persona o cosa; reconocimiento.
- **Autenticación.-** Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, se tiene o una combinación de todas.
- **Autorización.-** Lo que se permite cuando se ha otorgado acceso
- **No repudio.-** No se puede negar un evento o una transacción.
- **Seguridad en capas.-** La defensa a profundidad que contenga la inestabilidad
- **Control de Acceso.-** Limitar el acceso autorizado solo a entidades autenticadas
- **Métricas de Seguridad, Monitoreo.-** Medición de actividades de seguridad
- **Gobierno.-** Proporcionar control y dirección a las actividades
- **Estrategia.-** Los pasos que se requieren para alcanzar un objetivo
- **Arquitectura.-** El diseño de la estructura y las relaciones de sus elementos
- **Gerencia.-** Vigilar las actividades para garantizar que se alcancen los objetivos
- **Riesgo.-** La explotación de una vulnerabilidad por parte de una amenaza
- **Exposiciones.-** Áreas que son vulnerables a un impacto por parte de una amenaza
- **Vulnerabilidades.-** deficiencias que pueden ser explotadas por amenazas
- **Amenazas.-** Cualquier acción o evento que puede ocasionar consecuencias adversas
- **Riesgo residual.-** El riesgo que permanece después de que se han implementado contra medidas y controles
- **Impacto.-** Los resultados y consecuencias de que se materialice un riesgo
- **Sensibilidad.-** El nivel de impacto que tendría una divulgación no autorizada
- **Análisis de impacto al negocio.-** Evaluar los resultados y las consecuencias de la inestabilidad
- **Controles.-** Cualquier acción o proceso que se utiliza para mitigar el riesgo
- **Contra medidas.-** Cualquier acción o proceso que reduce la vulnerabilidad
- **Políticas.-** Declaración de alto nivel sobre la intención y la dirección de la gerencia
- **Normas.-** Establecer los límites permisibles de acciones y procesos para cumplir con las políticas
- **Ataques.-** Tipos y naturaleza de inestabilidad en la seguridad
- **Clasificación de Datos.-** El proceso de determinar la sensibilidad y Criticidad de la información

3.2. Contraseñas.

Aunque en la actualidad existen varias formas de autenticación de usuarios, la mayoría inician sesión en su equipo escribiendo una combinación del nombre de usuario y una contraseña mediante el teclado. Algunos productos emplean tecnologías más seguras como, por ejemplo, la biométrica, las tarjetas inteligentes y las contraseñas de un solo uso para todos los sistemas operativos más habituales. Sin embargo, la mayor parte de las organizaciones siguen confiando en las contraseñas y seguirán haciéndolo en los próximos años. A menudo, los usuarios disponen de varias cuentas de equipo en el trabajo, para el teléfono móvil, el banco, la compañía de seguros, etc. Con el fin de recordar las contraseñas con mayor facilidad, suelen utilizar contraseñas idénticas o parecidas para todas las cuentas. Las contraseñas cortas y sencillas constituyen un objetivo relativamente fácil para los atacantes.

3.3. Análisis de Riesgos

La información es el activo más importante que se posee hoy en día una empresa, y, por lo tanto, deben existir técnicas y métodos que le den seguridad, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo. Los medios para conseguirlo son:

- Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
- Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
- Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
- Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
- Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
- Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

3.4. Amenazas.

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguras, todavía deben ser tomadas en cuenta circunstancias que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables. Estos son causados por:

- **El usuario.-** Causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).
- **Programas maliciosos.-** Programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos, pueden ser un virus informático, un gusano informático, un troyano, o programa espía.
- **Un intruso.-** Persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker o hacker).
- **Un siniestro (robo, incendio, por agua).-** Una mala manipulación o una mal intención derivan a la pérdida del material o de los archivos.

3.5. Técnicas de Aseguramiento del Sistema.

Codificar la información: A través del uso de la Criptología[9], o contraseñas difíciles de averiguar a partir de datos personales del individuo.
Tecnologías repelentes o protectoras: Cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc.
Mantener con las actualizaciones: Los sistemas de información con las actualizaciones que más impacten en la seguridad.

3.5.1. Consideraciones de Software.

- Es recomendable tener instalado en la máquina únicamente el software necesario, ya que se reduce riesgos.
- Tener controlado el software asegura la calidad de la procedencia del mismo (el software obtenido de forma ilegal o sin garantías aumenta los riesgos). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre.

[9] La criptología es el estudio de los criptosistemas, sistemas que ofrecen medios seguros de comunicación en los que un emisor oculta o cifra un mensaje antes de transmitirlo para que sólo un receptor autorizado pueda descifrarlo

CAPITULO IV: AUDITORIA INFORMÁTICA

4.1. Definición.

Es la revisión y evaluación de los controles, sistemas, procedimientos de informática y de los equipos de cómputo[10], su utilización, eficiencia y seguridad, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría informática debe partir de una situación dada; ésta es metódica, puesto que seguirá un plan de trabajo perfectamente sistematizado que permite llegar a conclusiones suficientemente justificadas; es puntual y será ejecutada por personas ajenas al departamento independientes de las funciones a auditar.

4.2. Tipos de Auditoria Informática

Auditoría Informática de Explotación.- Auditar Explotación consiste en evaluar los datos, su transformación, los controles de integridad y calidad, y sus interrelaciones.

Auditoría Informática de Desarrollo de Proyectos o Aplicaciones.- Consiste en auditar aplicaciones en desarrollo, en sus diferentes fases, puesto que deben estar sometidas a un exigente control interno; caso contrario, además de la elevación de costos, podrá producirse la insatisfacción del usuario. Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la máquina sean exactamente los previstos y no otros.

Auditoría Informática de Sistemas.- Es el examen o revisión de carácter objetivo (independiente), crítico(evidencia), sistemático (normas), selectivo (muestras) de las políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con los sistemas de información computarizados, con el fin de emitir una opinión profesional (imparcial) con respecto a: eficiencia en el uso de los recursos informáticos, validez de la información y efectividad de los controles establecidos.

Auditoría de la Seguridad Informática.- Abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las

[10] Wikipedia, (2010) Auditoria Informática [en línea] Disponible en: http://es.wikipedia.org/wiki/Auditoria_informatica

situaciones de incendios, sabotaje, robos, catástrofes naturales, etc. La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

4.3. Proceso Metodológico para elaborar una Auditoría Informática

4.3.1. Diagnóstico.

Esta fase incluye a la alta dirección y las áreas usuarias. Se busca la opinión de la primera para saber el grado de satisfacción y confianza que tienen en los productos, servicios y recursos de informática en el negocio. Se detectan las fortalezas, aciertos, apoyo que brinda dicha función y las oportunidades que puede ofrecer la informática para hacer más competitivo el negocio.

Conocimiento del negocio.- El auditor en informática debe conocer: la misión, estrategias, planes, el nivel jerárquico de la función de informática y las entidades externas a la empresa que se relacionan con cada área de la misma.

Apoyo al negocio.- El auditor informático debe tener una idea global del grado de apoyo y satisfacción que existe en el negocio, y saber hacia donde se orienta el soporte de la función de informática.

Áreas de oportunidad.- Se detectan las características que van a facilitar la implementación de soluciones brindadas por informática y que tendrán gran impacto sobre alguna función del negocio. Las áreas de oportunidad deben ser analizadas y documentadas antes de ponerlas en práctica.

Diagnóstico de informática.- Aquí el auditor se coordina directamente con el responsable de la función de informática.

Conocimiento de la función de informática.- El auditor conocerá la estructura interna de informática, funciones, objetivos, estrategias, planes y políticas, para lo que se apoyará en la tecnología de software y hardware.

4.3.2. Etapa de Justificación.

El auditor se centrará en elaborar un documento fundamental para la aprobación del proyecto, el mismo que debe contemplar: las áreas que se auditarán (matriz de

riesgo), el tiempo sugerido para hacerlo (plan de auditoría informática) y el visto bueno (compromiso ejecutivo).

Matriz de riesgo.- El objetivo principal es detectar las áreas de mayor peligro en relación con informática y que requieren una revisión formal y oportuna y determinar el nivel de riesgo que existe en cada área detectada, para asegurar que se desarrolle de acuerdo con los estándares, políticas y procedimientos que se le asignaron según su función.

Plan de auditoría informática.- Consiste en plantear las tareas más importantes que se ejecutarán durante cierto período al efectuar la auditoría. Este plan se deriva de los siguientes elementos: Áreas de oportunidad, matriz de riesgos y las prioridades de la alta dirección, de auditoría y de informática.

Compromiso ejecutivo.- Su objetivo principal es obtener el visto bueno inicial de la alta dirección y demás responsables para continuar con el proyecto de auditoría.

4.3.3. Etapa de Adecuación.

Esta etapa es un conjunto de tareas estructuradas para que el proyecto de auditoría informática se adapte a las necesidades de la empresa estudiada, pero sin olvidar la referencia de los estándares, políticas y procedimientos de auditoría que siempre son aceptados y recomendados por las asociaciones relacionadas con el proceso. Los elementos que se deben contemplar son:

Objetivos y requerimientos de éxito por cada área que se auditará.- Se desarrolla tomando como base la matriz de riesgo. Debido a que a medida que avanza el proyecto, surgen cancelaciones, prioridades, requerimientos, expectativas, nuevos involucrados, etc., el auditor debe actualizar el plan de trabajo, detallar fechas, tiempos, resultados esperados, responsabilidades y funciones, así como estimar gastos y el número de personas que participarán.

Plan detallado del proyecto de auditoría informática.- Se define cada detalle de los elementos del proyecto; se especifican las tareas, productos terminados, responsables, fechas, etc., que serán validados y aprobados en la etapa de formalización para arrancar el proyecto. Hay dos tipos de planes detallados:

- Plan interno, que le corresponde al líder de proyecto y su propósito es hacer un seguimiento interno a las tareas y responsabilidades de los auditores.

- Plan detallado de auditoría en informática, en el que se especifica el detalle emanado del plan general de auditoría informática.

Definición de técnicas y herramientas.- Consiste en definir las técnicas y herramientas esenciales para revisar eficientemente cada área seleccionada.

Adecuación a la alta política de empresa.- Todas las tareas realizadas por la auditoría informática deben cumplir con los estándares, políticas y procedimientos establecidos por asociaciones profesionales y por las empresas donde se preste el servicio.

Elaboración de cuestionarios.- Se estructuran de manera que sirven de guía para verificar la confiabilidad de la información del personal entrevistado; además, permiten percibir el grado de cumplimiento de estándares, políticas y procedimientos que generalmente son aceptados.

4.3.4. Etapa de Formalización.

En esta etapa la alta dirección da su aprobación y apoyo formal para el desarrollo del proyecto de auditoría, de tal manera que, su función es justificar el desarrollo del proyecto basándose en lo que se hizo en las etapas anteriores.

Verificación de prioridades, restricciones y alcance del proyecto.- Permite la clarificación del rumbo, límites y cobertura que tendrá el proyecto.

Presentación formal del plan de auditoría informática.- Se justificará la continuidad del proceso, para lo cual el responsable de esta tarea deberá:

- Asegurarse de contar con toda la información resumida y presentable.
- Revisarla y verificarla.
- Concertar en una cita en una fecha y lugar apropiados.
- Ser fluido, claro y contundente en la presentación.

Aprobación formal del proyecto.- En esta tarea surge la aprobación formal del proyecto de auditoría.

Compromiso ejecutivo.- Lograr que la alta dirección, los usuarios clave, el responsable de informática y el de la auditoría se comprometan a lo largo del proyecto, desde ese momento hasta el desarrollo e implantación de las acciones recomendadas por auditoría informática en su informe final.

4.3.5. Etapa de Desarrollo.

El auditor informático comienza a ejecutar sus tareas de acuerdo con el plan aprobado en la etapa anterior. Esta fase comprende:

- Concertación de fechas de entrevistas, visitas y de aplicación de cuestionarios.
- Verificación de las tareas, involucrados y productos terminados.
- Clasificar técnicas y herramientas.
- Aplicación de entrevistas y cuestionarios.
- Efectuar visitas para la verificación.
- Elaboración de informes preliminares.
- Revisión de estos informes.
- Clasificación y documentación de los informes, para su correcta lectura.
- Finalización de tareas o productos pendientes.
- Elaboración del informe final de la auditoría informática.
- Presentación a la alta dirección e involucrados clave y aprobación del proyecto y compromiso ejecutivo.

4.3.6. Etapa de Implantación

En ésta fase los responsables de las áreas usuarias y de informática ejecutarán las acciones recomendadas en los informes aprobados por la alta dirección. La función del auditor es una labor de seguimiento y apoyo. Los elementos clave son:

- Definición de requerimientos para el éxito de la etapa de implantación.
- Desarrollo del plan de implantación.
- Implantación de las acciones sugeridas por auditoría en informática.
- Seguimiento a la implantación

4.4. Auditoria de Sistemas.

4.4.1. Objetivos Específicos.

- Evaluación de la seguridad en el área informática.
- Evaluación de suficiencia en los planes de contingencia: respaldos, prevención de acontecimientos.
- Opinión de la utilización de los recursos informáticos: resguardo y protección de activos.

- Control de modificación a las aplicaciones existentes: fraudes, control a las modificaciones de los programas.
- Revisión y control de la utilización del sistema operativo programas: utilitarios.
- Auditoría de la base de datos.
- El Análisis y control de la función informática (Sistema de Información - SI y la Tecnología de la Información -TI).
- La verificación del cumplimiento de la Normativa General de la Organización.
- La verificación de los Planes, Programas y Presupuestos de los Sistemas Informáticos.
- La revisión de la gestión de los recursos materiales y humanos informáticos.
- La revisión y verificación de las Seguridades: Cumplimiento de normas y estándares, Sistema Operativo, Seguridad de Software, Comunicaciones, Base de Datos, Aplicaciones, Seguridad Física, Suministros y Contingencias.
- El análisis del control de resultados.
- El análisis de verificación y de exposición de debilidades y disfunciones.

4.4.2. Fines de la Auditoria de Sistemas.

- Fundamentar la opinión del auditor interno (externo) sobre la confiabilidad de los sistemas de información.
- Expresar la opinión sobre la eficiencia de las operaciones en el área de TI.

4.4.3. Herramientas y Técnicas para la Auditoría de Sistemas.

- Cuestionarios y entrevistas
- Formularios checklist y virtuales.
- Pruebas de consistencias.
- Inventarios y valorizaciones.
- Historias de cambios y mejoras.
- Reporte de bases de datos, archivos y estándares utilizados.
- Compatibilidades e uniformidades.
- Software de interrogación:
- Certificados, garantías, otros del software.
- Fotografías o tomas de valor (Imágenes).
- Diseño de flujos y de la red de Información.
- Planos de distribución e instalación (Para Estudio y Revisión).
- Listado de proveedores, entre otros.

CAPITULO V: TECNOLOGÍAS PARA EL DESARROLLO DE LA APLICACIONES WEB

5.1. JSF

5.1.1. ¿Qué es JSF?

JavaServer Faces (JSF) es una tecnología y framework para aplicaciones Java basadas en web que simplifica el desarrollo de interfaces de usuario en aplicaciones Java. JSF usa JavaServer Pages (JSP) como la tecnología que permite hacer el despliegue de las páginas[11].

5.1.2. Características.

- Utiliza páginas JSP para generar las vistas, añadiendo una biblioteca de etiquetas propia para crear los elementos de los formularios HTML.
- Asocia a cada vista con formularios un conjunto de objetos java manejados por el controlador (managed beans) que facilitan la recogida, manipulación y visualización de los valores mostrados en los diferentes elementos de los formularios.
- Introduce una serie de etapas en el procesamiento de la petición, como por ejemplo la de validación, reconstrucción de la vista, recuperación de los valores de los elementos, etc.
- Utiliza un sencillo fichero de configuración para el controlador en formato xml
- Es extensible, pudiendo crearse nuevos elementos de la interfaz o modificar los ya existentes.
- Y lo que es más importante: forma parte del estándar J2EE. En efecto, hay muchas alternativas para crear la capa de presentación y control de una aplicación web java, pero solo JSP forma parte del estándar.

5.1.3. Ventajas de utilizar JSF:

- JSF nos permite desarrollar rápidamente aplicaciones de negocio dinámicas en las que toda la lógica de negocio se implementa en java, o es llamada desde java, creando páginas para las vistas muy sencillas.
- JSF resuelve validaciones, conversiones, mensajes de error e internacionalización.

[11] Wikipedia, (2010) JavaServer Faces [en línea] Disponible en: http://es.wikipedia.org/wiki/JavaServer_Faces

- JSF se integra dentro de la página JSP[12] y se encarga de la recogida y generación de los valores de los elementos de la página
- JSF permite introducir javascript en la página, para acelerar la respuesta de la interfaz en el cliente (navegador del usuario).
- JSF es extensible, por lo que se pueden desarrollar nuevos componentes a medida, También se puede modificar el comportamiento del framework mediante APIs que controlan su funcionamiento.

5.1.4. Que contiene JSF:

- Páginas JSP que incluyen los formularios JSF. Estas páginas generarán las vistas de la aplicación.
- Beans java que se conectan con los formularios JSF.
- Clases java para la lógica de negocio y utilidades.
- Ficheros de configuración, componentes a medida y otros elementos del framework.
- Un modelo de eventos en el lado del servidor.
- Resto de recursos de la aplicación web: recursos estáticos, javascript y otros elementos.
- Una librería de etiquetas JavaServer Pages (JSP) personalizadas para dibujar componentes UI dentro de una página JSP.
- Un conjunto de APIs para representar componentes de una interfaz de usuario y administrar su estado, manejar eventos, validar entrada, definir un esquema de navegación de las páginas y dar soporte para internacionalización y accesibilidad.
- Dos bibliotecas de etiquetas personalizadas para Java Server Pages que permiten expresar una interfaz Java Server Faces dentro de una página JSP.

5.1.5. El Ciclo de Vida de una Página Java Server Faces.

El ciclo de vida de una página JavaServer Faces es similar al de una página JSP: El cliente hace una petición HTTP de la página y el servidor responde con la página traducida a HTML. Sin embargo, debido a las características extras que ofrece la tecnología JavaServer Faces, el ciclo de vida proporciona algunos servicios adicionales mediante la ejecución de algunos pasos extras.

[12] **JSP** (Página de Servidor Java): Es un tipo especial de página

Los pasos del ciclo de vida que se ejecutan dependen si la petición se originó o no desde una aplicación JSF y si la respuesta es o no generada con la fase de renderizado del ciclo de vida de JSF.

5.1.6. Escenarios de Procesamiento del Ciclo de Vida de una Petición

Una aplicación JavaServer Faces soporta dos tipos de respuestas y peticiones:

- **Respuesta Faces:** Una respuesta servlet que se generó mediante la ejecución de la fase Renderizar la respuesta del ciclo de vida de procesamiento de la respuesta.
- **Respuesta No-Faces:** Una respuesta servlet que no se generó mediante la ejecución de la fase Renderizar la Respuesta. Un ejemplo es una página JSP que no incorpora componentes JavaServer Faces.
- **Petición Faces:** Una petición servlet que fue enviada desde una Respuesta Faces previamente generada. Un ejemplo es un formulario enviado desde un componente de interface de usuario JSF, donde la URL de la petición identifica el árbol de componentes JSF para usar el procesamiento de petición.
- **Petición No-Faces:** Una petición servlet que fue enviada a un componente de aplicación como un servlet o una página JSP, en vez de directamente a un componente JavaServer Faces.

La combinación de estas peticiones y respuestas resulta en tres posibles escenarios del ciclo de vida que pueden existir:

- **Escenario 1: Una Petición No-Faces genera una Respuesta Faces**:

  Un ejemplo de este escenario es cuando se pulsa un enlace de una página HTML que abre una página que contiene componentes JavaServer Faces. Para dibujar una Respuesta Faces desde una petición No-Faces, una aplicación debe proporcionar un mapeo FacesServlet en la URL de la página que contiene componentes JSF. FacesServlet acepta la petición entrante y pasa a la implementación del ciclo de vida para su procesamiento.

- **Escenario 2: Una Petición Faces genera una Respuesta No-Faces**:

  Algunas veces una aplicación JavaServer Faces podría necesitar redirigir la salida a un recurso diferente de la aplicación Web diferente o generar una

respuesta que no contiene componentes JavaServer Faces. En estas situaciones, el desarrollador debe saltarse la fase de renderizado (Renderizar la Respuesta) llamando a FacesContext.responseComplete. FacesContext contiene toda la información asociada con una Petición Faces particular. Este método se puede invocar durante las fases Aplicar los Valores de Respuesta, Procesar Validaciones o Actualizar los Valores del Modelo.

- **Escenario 3: Una Petición Faces genera una Respuesta Faces**:

Es el escenario más común en el ciclo de vida de una aplicación JavaServer Faces. Este escenario implica componentes JavaServer Faces enviando una petición a una aplicación JavaServer Faces utilizando el FacesServlet. Como la petición ha sido manejada por la implementación JavaServer Faces, la aplicación no necesita pasos adicionales para generar la respuesta.

5.1.7. Ciclo de Vida Estándar de Procesamiento de Peticiones - Respuesta

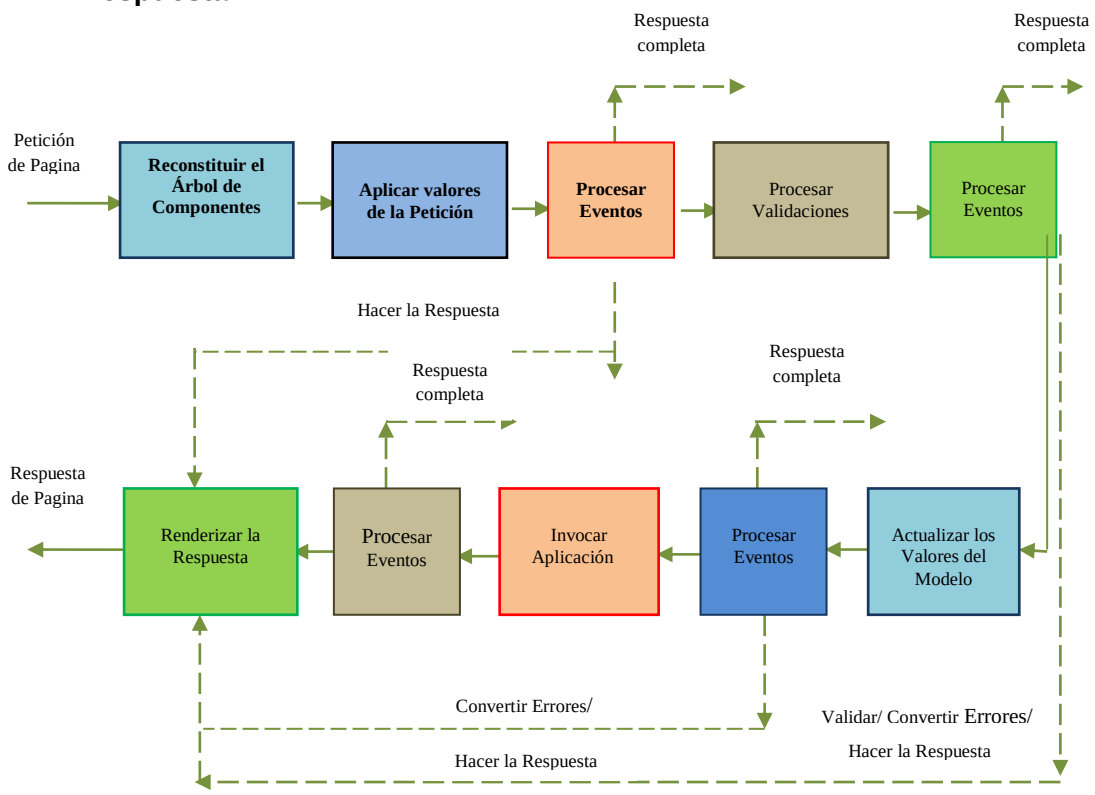


Fig. 5. Ciclo de Vida de JavaServer Faces

- **Reconstituir el Árbol de Componentes**

Cuando se hace una petición para una página JavaServer Faces, como cuando se pulsa sobre un enlace o un botón, la implementación JavaServer Faces comienza el estado (Reconstituir el Árbol de Componentes).

Durante esta fase, la implementación JavaServer Faces construye el árbol de componentes de la página JavaServer Faces, conecta los manejadores de eventos y los validadores y graba el estado en el FacesContext.

- **Aplicar Valores de la Petición**

Una vez construido el árbol de componentes, cada componente del árbol extrae su nuevo valor desde los parámetros de la petición con su método decode. Entonces el valor es almacenado localmente en el componente. Si falla la conversión del valor, se genera un mensaje de error asociado con el componente y se pone en la cola de FacesContext. Este mensaje se mostrará durante la fase (Renderizar la Respuesta), junto con cualquier error de validación resultante de la fase (Procesar Validaciones).

Si durante esta fase se produce algún evento, la implementación JavaServer Faces emite los eventos a los oyentes interesados.

- **Procesar Validaciones**

Durante esta fase, la implementación JavaServer Faces procesa todas las validaciones registradas con los componentes del árbol. Examina los atributos del componente que especifican las reglas de validación y compara esas reglas con el valor local almacenado en el componente. Si el valor local no es válido, la implementación JavaServer Faces añade un mensaje de error al FacesContext y el ciclo de vida avanza directamente hasta la fase (Renderizar las Respuesta) para que la página sea dibujada de nuevo incluyendo los mensajes de error. Si había errores de conversión de la fase (Aplicar los Valores a la Petición), también se mostrarán.

En este momento, si la aplicación necesita redirigirse a un recurso de aplicación Web diferente o generar una respuesta que no contenga componentes JavaServer Faces. Si se han disparado eventos durante esta fase, la implementación JavaServer Faces los emite a los oyentes interesados.

- **Actualizar los Valores del Modelo**

Una vez que la implementación JavaServer Faces determina que el dato es válido, puede pasar por el árbol de componentes y configurar los valores del objeto de modelo correspondiente con los valores locales de los componentes. Sólo se actualizarán los componentes que tengan expresiones valueRef. Si el dato local no se puede convertir a los tipos especificados por las propiedades del objeto del modelo, el ciclo de vida avanza directamente a la fase (Renderizar las Respuesta), durante la que se dibujará de nuevo la página mostrando los errores, similar a lo que sucede con los errores de validación.

- **Invocar Aplicación**

Durante esta fase, la implementación JavaServer Faces maneja cualquier evento a nivel de aplicación, como enviar un formulario o enlazar a otra página.

Luego la implementación JavaServer Faces configura el árbol de componentes de la respuesta a esa nueva página. Finalmente, la implementación JavaServer Faces transfiere el control a la fase (Renderizar la Respuesta).

- **Renderizar la Respuesta**

Durante esta fase, la implementación JavaServer Faces invoca las propiedades de codificación de los componentes y dibuja los componentes del árbol de componentes grabado en el FacesContext. Si se encontraron errores durante las fases (Aplicar los Valores a la Petición, Procesar Validaciones o Actualizar los Valores del Model), se dibujará la página original. Si las páginas contienen etiquetas output_errors, cualquier mensaje de error que haya en la cola se mostrará en la página.

5.2. JASPER REPORTS

5.2.1. Definición

JasperReports es una herramienta que se compone de un conjunto de librerías java para facilitar la generación de informes en nuestras aplicaciones tanto web como de escritorio[13]. Para utilizar JasperReports es necesario añadirlo a las aplicaciones Java por medio de la inclusión de su librería al classpath de la aplicación. Los informes se

[13] Sanromán, J, (2007) ¿Que es Jasper Reports? [en línea] Disponible en: http://www.jsanroman.net/2007/11/20/%C2%BFque-es-jasper-reports-2/

definen en un fichero xml el cual será compilado por las librerías jasperReport y generarán un fichero .jasper que utilizaremos para rellenar y mostrar el informe final.

La salida de los informes puede ser a la impresora, pdf, cvs, xml, txt, html, xls, rtf, jasper viewer. JasperReports se usa comúnmente con iReport.

5.2.2. Características de JasperReports

- Además de los datos en texto, JasperReports permite incluir en los reportes imágenes, gráficos, etc., para que los mismos tengan un aspecto profesional.
- Permite una diagramación flexible de los reportes: Los reportes se pueden dividir en secciones opcionales que son: titulo del reporte, el encabezado de página, una sección para los detalles del reporte, el pie de página y una sección de resumen que aparece al final del reporte.
- Permite que los desarrolladores le surtan datos en varias formas: esto es que los desarrolladores pueden pasar datos a los reportes por medio del paso de parámetros. Estos parámetros de reportes pueden ser instancia de cualquier clase de Java.
- Pueden generar sub-reportes: JasperReports permite la creación de reportes dentro de reportes lo que facilita bastante el diseño porque es posible usar estos sub-reportes en otros reportes.
- No sólo son capaces de mostrar los datos que le son pasados sino que pueden generar o calcular con esos datos otros datos de forma dinámica y mostrarlos.
- Pueden generar marcas de agua: JasperReports permite generar textos o imágenes de fondo para utilizarlo como marcas de agua con el propósito de identificar el reporte o simplemente por motivos de seguridad.
- Se pueden exportar los reportes a una multitud de formatos: Los reportes generados con JasperReports pueden ser exportados a una multitud de formatos como PDF, XLS, RTF, HTML, XML, CVS (valores separados por coma) y texto plano.

5.2.3. Funcionamiento

JasperReports trabaja en forma similar a un compilador y a un intérprete. El usuario diseña el reporte codificándolo en XML de acuerdo a las etiquetas y atributos definidos en un archivo llamado jasperreports.dtd (parte de JasperReports). Usando XML el usuario define completamente el reporte, describiendo donde colocar texto, imágenes,

líneas, rectángulos, cómo adquirir los datos, como realizar ciertos cálculos para mostrar totales, etc.

Este archivo fuente XML debe ser compilado para obtener un reporte real. La versión compilada del fuente es nombrada "archivo jasper" (este termina con .jasper). Un archivo jasper es el compilado de un código fuente. Cuando tenemos un archivo jasper, necesitamos otra cosa para producir un reporte: necesitamos datos. Esto no siempre es cierto. En algunos casos querríamos generar un reporte que no mostrara datos dinámicos, solo texto estático por ejemplo, pero esto puede simplificarse a un reporte que tiene solamente un registro vacío. Para proporcionar estos registros al "jasper engine" necesitamos presentarlos usando una interfaz especial específica llamada JRDataSource. Una fuente de datos + un Archivo jasper = un "archivo print". Un "archivo print" puede exportarse en muchos formatos como PDF, HTML, RTF, XML, XLS, CVS, etc. La exportación se puede realizar utilizando clases especiales para implementar exportadores específicos.

5.2.4. Proceso de creación de un Reporte

Cuando se trabaja con JasperReports los pasos en el proceso de creación de un reporte son los siguientes:

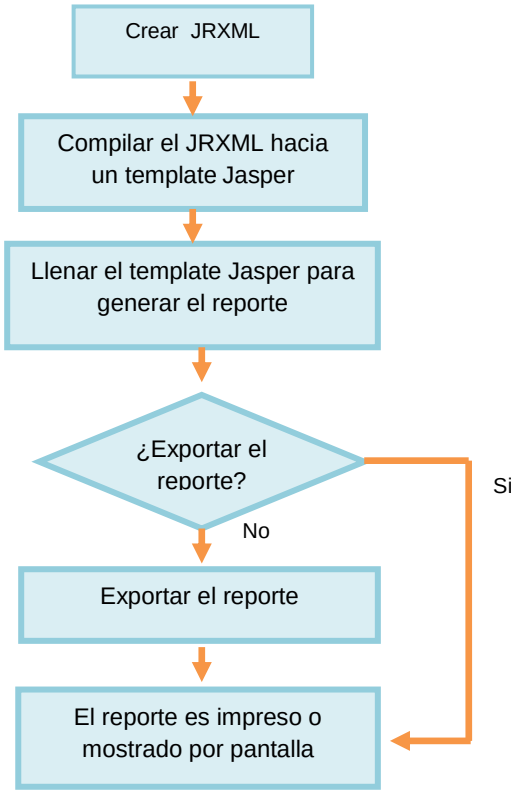


Fig. 6. Proceso de Creación de un Reporte

5.3. IREPORT

5.3.1. Definición

La herramienta iReport es un constructor / diseñador de informes visual, poderoso, intuitivo y fácil de usar para JasperReports escrito en Java. Este instrumento permite que los usuarios corrijan visualmente informes complejos con cartas, imágenes, subinformes, etc. iReport está además integrado con JFreeChart, una de la biblioteca gráficas OpenSource más difundida para Java. Los datos para imprimir pueden ser recuperados por varios caminos, TableModels, JavaBeans, XML, etc.

5.3.2. Características de iReport

La lista siguiente describe algunas de las características importantes de iReport:

- 100% escrito en JAVA y además OPENSOURCE.
- Maneja el 98% de las etiquetas de JasperReports
- Permite diseñar con sus propias herramientas: rectángulos, líneas, elipses, campos de texto, cartas, subreportes.
- Soporta internacionalización nativamente.
- Browser de la estructura del documento.
- Recopilador y exportador integrados.
- Soporta JavaBeans como orígenes de datos (éstos deben implementar la interface JRDataSource).
- Incluye Wizard's (asistentes) para crear automáticamente informes.
- Tiene asistentes para generar los subreportes
- Tiene asistentes para las plantillas.

5.4. ICEFACES

5.4.1. Definición

ICEfaces es un framework Ajax de Software Libre que utiliza las tecnologías Java EE para crear los componentes web de la interfaz para JSF. Permite utilizar técnicas Ajax de forma transparente, con un esfuerzo mínimo en Java/JSF, una de las características más interesantes es que es full Ajax, no es necesario configurar algo adicional ni estar tratando con varios archivos xml de configuración solamente es necesario instalar el plugin para Netbeans o Eclipse

5.4.2. Características.

- ICEfaces es considerado un framework que integra funcionalidad AJAX y permite a los desarrolladores Java EE, crear aplicaciones de una manera sencilla.
- Las aplicaciones desarrolladas en ICEfaces no necesitan plugins de navegador o applets para ser vistas.
- Estas aplicaciones están basadas en JavaServer Faces (JSF), así que permite el desarrollo de aplicaciones Java EE.
- Con la llegada de JSF, se empezó a vislumbrar posibilidades de integración.
- Sin embargo, de estas propuestas, ICEFaces fue una de las más acogidas ya que aísla completamente al desarrollador de AJAX. No hacen falta etiquetas especiales: se ponen los controles en la pantalla e ICEFaces se encarga de enviar entre cliente y servidor sólo la información necesaria.

5.4.3. Ventajas

Las ventajas del uso de ICEfaces para enriquecer las aplicaciones web de escritorio son numerosa. Debido a la cantidad de frameworks existentes, se procede a mostrar una serie de características diferenciadoras respecto a otros frameworks:

- **Experiencia de usuario enriquecedora:** crea una experiencia de usuario superior además de utilizar las ventajas de aplicaciones Java EE. Esto se consigue gracias a los componentes que vienen incluidos dentro de la distribución de ICEfaces.
- **Está basado en código abierto:** ICEfaces es un framework basado en Ajax bajo licencia de código abierto. La comunidad de desarrolladores de ICEfaces incluye cerca de 20.000 desarrolladores en 36 países.
- **Basado en estándares:** ICEfaces es una solución basada en Java, así que los desarrolladores pueden continuar trabajando de la misma forma que lo hacen. Hay multitud de plugins desarrollados para que ICEfaces sea integrado con multitud de IDEs Java.
- **El Ajax es transparente:** ICEfaces aporta a los programadores un desarrollo con mínimo esfuerzo en la sección JSF.
- **Compatibilidad:** ICEfaces soporta todos los servidores de aplicaciones, aporta plugins para los distintos IDEs y efectos javascript de librerías de cualquier empresa que haya desarrollado Ajax del mercado.

- **Seguridad:** ICEfaces es una de las soluciones Ajax más seguras del mercado. Es compatible con SSL, previene los scripts de cross-site, inyección de código malicioso. Es una solución Ajax basada en servidor, la cual no utiliza datos de usuarios, además es especialmente efectivo en la prevención de fallos en los submits de los formularios y el ataque SQL por inyección.
- **Escalabilidad y clustering:** El servidor asíncrono HTTP (AHS) aporta una alta escalabilidad para aplicaciones ICEfaces y pueden ser utilizadas por un gran número de usuarios concurrentes, además aporta despliegue en clúster (un requisito crítico que algunas soluciones no aportan).
- Carga de páginas incremental con edición de secciones y sin recargas de página completas.
- Se preserva el contexto del usuario durante la actualización de la página, incluyendo posición del foco y scroll.
- En aplicaciones de tiempo real, las recargas de páginas son asíncronas.

5.5. APACHE TOMCAT

5.5.1. Definición

Tomcat es un contenedor de Servlets con un entorno JSP. Un contenedor de Servlets es un shell de ejecución que maneja e invoca servlets por cuenta del usuario[14] . Incluye el compilador Jasper, que compila JSPs convirtiéndolas en servlets. El motor de servlets de Tomcat a menudo se presenta en combinación con el servidor web Apache.

Tomcat puede funcionar como servidor web por sí mismo, es usado como servidor web autónomo en entornos con alto nivel de tráfico y alta disponibilidad. Dado que Tomcat fue escrito en Java, funciona en cualquier sistema operativo que disponga de la máquina virtual Java.

5.5.2. Estructura de directorios Tomcat

Asumiendo que hemos descomprimido la distribución binaria de Tomcat deberíamos tener la siguiente estructura de directorios:

[14] Wikipedia, (2010) Tomcat [en línea] Disponible en: http://es.wikipedia.org/wiki/Apache_Tomcat

Nombre de Directorio	Descripción
Bin	Contiene los scripts de arrancar/parar
Conf	Contiene varios ficheros de configuración incluyendo server.xml (el fichero de configuración principal de Tomcat) y web.xml que configura los valores por defecto para las distintas aplicaciones desplegadas en Tomcat.
Doc	Contiene varia documentación sobre Tomcat.
Lib	Contiene varios ficheros jar que son utilizados por Tomcat. Sobre UNIX, cualquier fichero de este directorio se añade al classpath de Tomcat.
Logs	Aquí es donde Tomcat sitúa los ficheros de diario.
Src	Los ficheros fuentes del API Servlet. ¡No te excites, todavía! Esto son sólo los interfaces vacíos y las clases abstractas que debería implementar cualquier contenedor de servlets.
webapps	Directorio que web contiene aplicaciones Web de Ejemplo.
Work	Generado automáticamente por Tomcat, este es el sitio donde Tomcat sitúa los ficheros intermedios (como las páginas JSP compiladas) durante su trabajo. Si borramos este directorio mientras se está ejecutando Tomcat no podremos ejecutar páginas JSP.
Clases	Podemos crear este directorio para añadir clases adicionales al classpath. Cualquier clase que añadamos a este directorio encontrará un lugar en el classpath de Tomcat

Tabla 5. Directorios de Tomcat

5.5.3. Ficheros de Configuración de Tomcat

La configuración de Tomcat se basa en dos ficheros:

1. **server.xml -** El fichero de configuración global de Tomcat.
2. **web.xml -** Configura los distintos contextos en Tomcat.

5.6. HTML

5.6.1. Definición

HTML es el lenguaje con el que se escriben las páginas web. Las páginas web pueden ser vistas por el usuario mediante un tipo de aplicación llamada navegador. Podemos

decir por lo tanto que el HTML es el lenguaje usado por los navegadores para mostrar las páginas webs al usuario, siendo hoy en día la interface más extendida en la red[15].

Este lenguaje nos permite aglutinar textos, sonidos e imágenes y combinarlos a nuestro gusto. Además, y es aquí donde reside su ventaja con respecto a libros o revistas, el HTML nos permite la introducción de referencias a otras páginas por medio de los enlaces hipertexto.

5.6.2. Elementos de HTML

Podemos agrupar los elementos de HTML en los siguientes grupos:

- Estructura
- Texto
- Listas
- Tablas
- Vínculos
- Objetos
- Estilo
- Marcos
- Formularios
- Scripts

5.6.3. Partes de un documento HTML

Además de todo esto, un documento HTML ha de estar delimitado por la etiqueta **<html> y </html>**. Dentro de este documento, podemos asimismo distinguir dos partes principales:

- **El encabezado, delimitado por <head> y </head>** donde colocaremos etiquetas de índole informativo como por ejemplo el titulo de nuestra página.
- **El cuerpo, flanqueado por las etiquetas <body> y </body>**, que será donde colocaremos nuestro texto e imágenes delimitados a su vez por otras etiquetas como las que hemos visto.

  El resultado es un documento con la siguiente estructura:

[15]Super Hosting, (2000) Introducción al HTML [en línea] Disponible en: http://www.superhosting.cl/manuales/introduccion-al-html.html

<html>

<head>

- Etiquetas y contenidos del encabezado.
- Datos que no aparecen en nuestra página pero que son importantes para catalogarla: Titulo, palabras clave

</head>

<body>

- Etiquetas y contenidos del cuerpo.
- Parte del documento que será mostrada por el navegador: Texto e imágenes.

</body>

</html>

5.7. MYSQL

5.7.1. Definición

MySQL es un sistema de gestión de bases de datos relacional, licenciado bajo la GPL de la GNU. Su diseño multihilo le permite soportar una gran carga de forma muy eficiente. MySQL fue creada por la empresa sueca MySQL AB, que mantiene el copyright del código fuente del servidor SQL, así como también de la marca.

Aunque MySQL es software libre, MySQL AB distribuye una versión comercial de MySQL, que no se diferencia de la versión libre más que en el soporte técnico que se ofrece, y la posibilidad de integrar este gestor en un software propietario, ya que de no ser así, se vulneraría la licencia GPL.

Este gestor de bases de datos es, probablemente, el gestor más usado en el mundo del software libre, debido a su gran rapidez y facilidad de uso. Esta gran aceptación es debida, en parte, a que existen infinidad de librerías y otras herramientas que permiten su uso a través de gran cantidad de lenguajes de programación, además de su fácil instalación y configuración.

5.7.2. Características

Las principales características de este gestor de bases de datos son las siguientes:

- Aprovecha la potencia de sistemas multiprocesador, gracias a su implementación multihilo.
- Soporta gran cantidad de tipos de datos para las columnas.
- Dispone de API's en gran cantidad de lenguajes (C, C++, Java, PHP, etc).
- Gran portabilidad entre sistemas.
- Soporta hasta 32 índices por tabla.
- Gestión de usuarios y passwords, manteniendo un muy buen nivel de seguridad en los datos.
- Posibilidad de crear y configurar usuarios, asignando a cada uno de ellos permisos diferentes.
- Facilidad de exportación e importación de datos, incluso de la base de datos completa.
- Posibilidad de ejecutar conjuntos de instrucciones guardadas en ficheros externos a la base de datos.

5.7.3. Ventajas y Desventajas

Ventajas

- Velocidad al realizar las operaciones, lo que le hace uno de los gestores con mejor rendimiento.
- Bajo costo en requerimientos para la elaboración de bases de datos, ya que debido a su bajo consumo puede ser ejecutado en una máquina con escasos recursos sin ningún problema.
- Facilidad de configuración e instalación.
- Soporta gran variedad de Sistemas Operativos
- Baja probabilidad de corromper datos, incluso si los errores no se producen en el propio gestor, sino en el sistema en el que está.
- Conectividad y seguridad

Desventajas

- Un gran porcentaje de las utilidades de MySQL no están documentadas.
- No es intuitivo, como otros programas (ACCESS).
- Carece de soporte para transacciones, rollback's y subconsultas.
- El hecho de que no maneje la integridad referencial, hace de este gestor una solución pobre para muchos campos de aplicación, sobre todo para aquellos

programadores que provienen de otros gestores que sí que poseen esta característica.

- No es viable para su uso con grandes bases de datos, a las que se acceda continuamente, ya que no implementa una buena escalabilidad.

5.8. PATRÓN MODELO VISTA CONTROLADOR

5.8.1. Definición

El patrón Modelo Vista Controlador es un patrón de diseño orientado a objetos. Fue desarrollado en el Centro de Investigaciones Xerox Palo Alto a finales de los años setenta, tiene definida una buena arquitectura para un sitio web, además de especificar el uso de clases para dividir nuestra aplicación:

- Lógica del negocio -> datos persistentes
- Lógica de presentación -> como visualizamos los datos
- Flujo de la aplicación -> a través del controlador

5.8.2. Estructura

Modelo.- Está definido por el conjunto de clases y objetos correspondientes al Modelo del Negocio para nuestra aplicación (estados y funcionalidad), además es deseable un bajo acoplamiento con Vistas y Controladores

Por otro lado se definen métodos para realizar consultas (informar el estado), comandos (modificar el estado) y mecanismos de notificación (para informar a los observadores / vistas)

Vista.- Se encarga de administrar la visualización y presentación de la información, observa al Modelo para actualizar los cambios. Al definirse en el modelo una interfaz clara y estable, es fácil implementar múltiples Vistas para un mismo modelo, lo cual conlleva a que sea muy dependiente del Modelo (debe conocerlo), así como también dependiente del dispositivo y tecnología de visualización.

Controlador.- Es el responsable de definir el comportamiento de la aplicación, ya que recibe los eventos del usuario y decide qué es lo que se debe hacer, mapeándolos en comandos (mensajes) hacia el Modelo. Es altamente dependiente de los dispositivos y mecanismos de interacción del usuario y también muy dependiente del Modelo (debe conocerlo)

5.8.3. Esquema del Patrón Modelo Vista Controlador

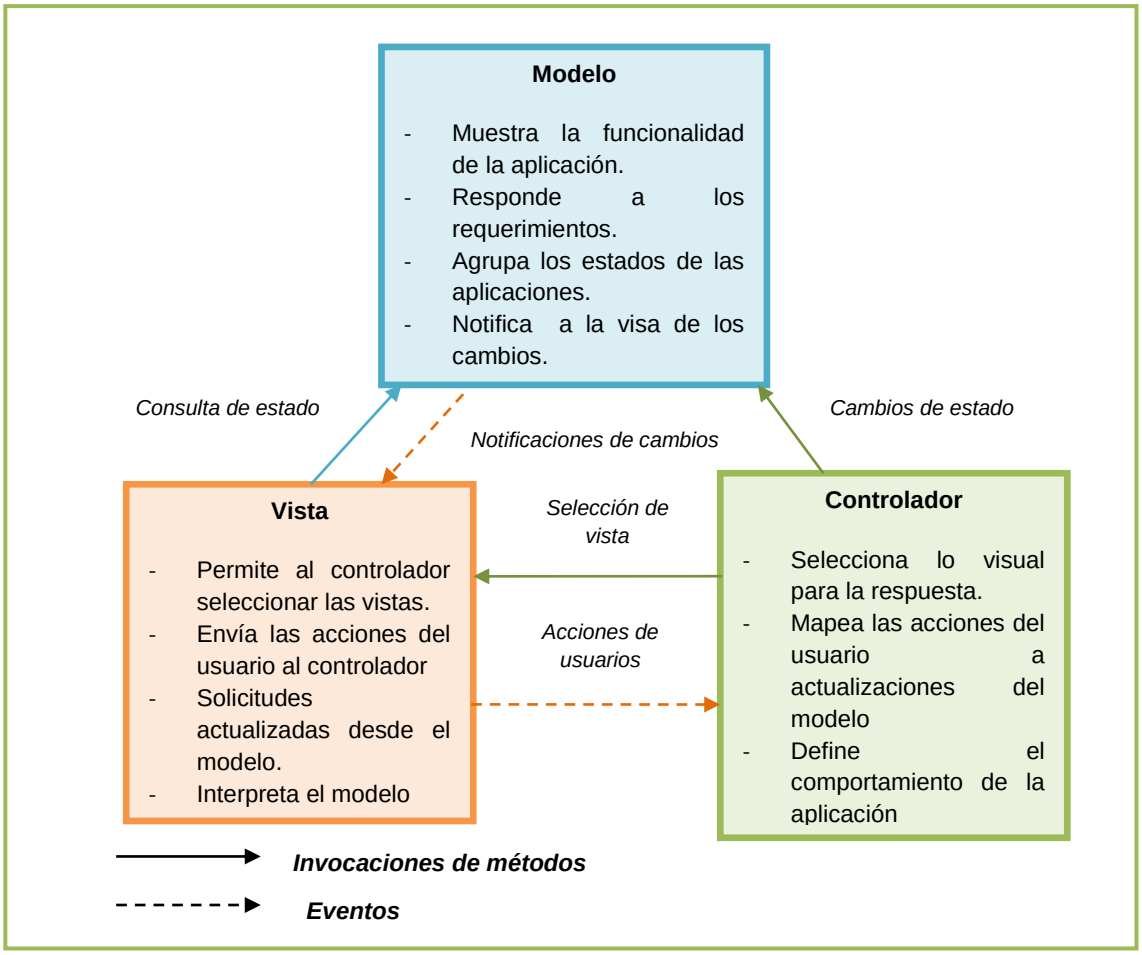


Fig. 7. Esquema del patrón Modelo Vista Controlador

5.8.4. Funcionamiento

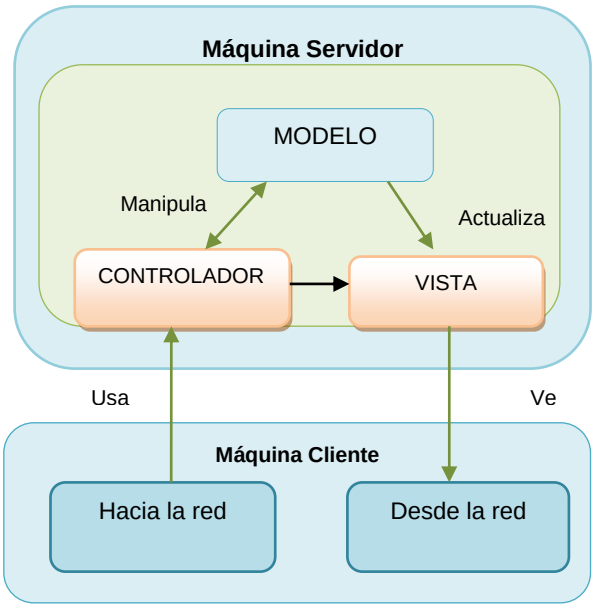


Fig. 8. Funcionamiento del Patrón Modelo Vista Controlador

5.8.5. Ventajas del Modelo Vista Controlador

Este modelo de arquitectura presenta varias ventajas:

- Hay una clara separación entre los componentes de un programa; lo cual nos permite implementarlos por separado es decir:
  - ✓ Desacopla las vistas de los modelos.
  - ✓ Desacopla los modelos de la forma en que se muestran e ingresan los datos.
- La conexión entre el Modelo y sus Vistas es dinámica; se produce en tiempo de ejecución, no en tiempo de compilación.
- Mayor cohesión.
  - ✓ Cada elemento del patrón está altamente especializado en su tarea (la vista en mostrar datos al usuario, el controlador en las entradas y el modelo en su objetivo de negocio).
- Las vistas proveen mayor flexibilidad y agilidad.
  - ✓ Se puede crear múltiples vistas de un modelo.
  - ✓ Las vistas pueden anidarse.
  - ✓ Se puede cambiar el modo en que una vista responde al usuario sin cambiar su representación visual.
  - ✓ Se puede sincronizar las vistas.
  - ✓ Las vistas pueden concentrarse en diferentes aspectos del modelo.
- Mayor facilidad para el desarrollo de clientes ricos en múltiples dispositivos y canales
  - ✓ Una vista para cada dispositivo que puede variar según sus capacidades.
  - ✓ Una vista para la Web y otra para aplicaciones de escritorio.
- Más claridad de diseño.
- Facilita el mantenimiento.
- Mayor escalabilidad.

CAPITULO VI: ILUSTRE MUNICIPIO DE CALVAS

6.1. Historia.

Calvas, en la época precolombina constituyó la nación indígena Curimanga y luego en la colonia la provincia de Calvas, la misma que comprendía los territorios de los actuales cantones: Macara, Calvas y parte de Gonzanamá, en la época de la Gran Colombia, el antiguo pueblo y asiento de Cariamanga fué elevado a la categoría de villa y cabecera cantonal.

El 25 de junio de 1824, El Excelentísimo Vicepresidente de la Gran Colombia, encargado del poder ejecutivo, Francisco de Paula Santander, impone el ejecútese, al decreto promulgado por la Cámara y El Senado reunidos en congreso, mediante el cual se establece la división territorial de la Gran Colombia. Y en el párrafo segundo del artículo 12 del mencionado decreto se crea el cantón Cariamanga como parte de la jurisdicción de la Provincia de Loja. En aquel entonces, el cantón Cariamanga comprendía los territorios del actual cantón Calvas, de los de Macará y parte de los de Gonzanamá, y estaba formado por las parroquias: Cariamanga, Sozoranga, Macará y Amaluza, siendo Cariamanga la cabecera cantonal del cantón Cariamanga. (hoy Calvas).

En 1830 El Gobierno de la República del Ecuador ratifica la creación del cantón Cariamanga, hecha en época de la gran Colombia en 1824. El Gobierno Federal de Loja, en octubre de 1859, decreta la división territorial y política de la provincia de Loja en cinco cantones, siendo uno de ellos el de Calvas. El cantón Calvas fue creado el 14 de Octubre de 1863, en la Presidencia del Dr. Gabriel García Moreno.

6.2. Base Legal

Su vida jurídica se encuentra basada y normada en las siguientes disposiciones legales:

a) Constitución Política de la República del Ecuador
b) Ley Orgánica de Régimen Municipal
c) Ley Orgánica de la Contraloría General del Estado
d) Ley Orgánica de Servicio Civil y Carrera Administrativa, y de Unificación y Homologación de las Remuneraciones del Sector Público.
e) Ley de Descentralización del Estado y de Participación Social

f) Ordenanzas

g) Demás leyes, reglamentos, normas y más disposiciones legales

6.3. Misión

El Ilustre Municipio del Cantón Calvas, fue creado mediante decreto de la división territorial y política de la provincia de Loja, expedido por el Sr. Manuel Carrión Pinzado, el 15 de octubre del año 1859, para satisfacer las necesidades colectivas del vecindario, especialmente las derivadas de la convivencia humana, cuya atención no compete a otros organismos gubernativos.

6.4. Visión

En el 2013 el Municipio del cantón Calvas logrará satisfacer las necesidades de los habitantes del cantón Calvas en el ámbito, social, cultural, deportivo, etc. Que garantice una mejor calidad de vida a su población.

6.5. Objetivos Estratégicos

- Procurar el bienestar material y social de la colectividad y contribuir al fomento y protección de los intereses locales.
- Planificar e impulsar el desarrollo físico del cantón y sus áreas urbanas y rurales.
- Acrecentar el espíritu de nacionalidad, el civismo y la confraternidad de los asociados, para lograr el creciente, progreso y la indisoluble unidad de la Nación; y,
- Promover el desarrollo económico, social, medio ambiental y cultural dentro de su jurisdicción

6.6. Objetivos Operativos

- Construcción, mantenimiento, aseo, embellecimiento y reglamentación del uso de caminos, calles, parques, plazas y demás espacios públicos.
- Recolección, procesamiento o utilización de residuos;
- Dotación y mantenimiento del alumbrado público;

6.7. Estructura Programática

Fig. 9. Estructura Programática del Ilustre Municipio de Calvas

6.8. Servicios Generales

6.8.1. Administración General

a) Asesoría Jurídica

A la Asesoría Jurídica junto con el Alcalde representará judicial y extrajudicialmente a la municipalidad, le corresponderá emitir dictámenes legales, elaboración y revisión de contratos, informes de actas, patrocinar defensa de juicios, preparar resoluciones, estudiar, organizar y actualizar la legislación que le corresponde conocer al concejo.

b) Del Secretario del Concejo

Al Secretario (a) del concejo le compete, dar fe de los actos del concejo, de la comisión de mesa y del alcalde; redactar y suscribir las actas de las sesiones del concejo y de la comisión de mesa; y las demás atribuciones que le otorga la Ley Orgánica de Régimen Municipal.

c) Del Auditor Interno

De conformidad a lo que señala la ley orgánica de régimen municipal, en las municipalidades habrá un auditor interno que será designado por el concejo, de una terna de fuera de su seno presentada por el alcalde. La designación del auditor (a) será para cuatro años y no excederá del plazo previsto para el alcalde en sus funciones, sin perjuicio de que el concejo pueda removerlo por causa justificada de acuerdo con la Ley.

d) De la Unidad de Informática

Al técnico de sistemas, le corresponderá el mantenimiento de los equipos de informática que posee el municipio para sus diferentes departamentos, capacitación de manejo de software al personal institucional, asesoramiento y asistencia técnica a todas las Unidades Administrativas y Operativas de la municipalidad, y las demás actividades señaladas en el orgánico funcional, así como de las actividades que el señor alcalde le disponga.

e) De la Unidad de Recursos Humanos

A la unidad de recursos humanos, le corresponderá el control de asistencia, generación de vacaciones, acciones de personal (ingresos y salidas), coordinación de capacitación institucional y demás funciones constantes en el orgánico funcional, de la misma manera que deberá hacer cumplir la ley

orgánica de servicio civil y carrera administrativa, código de trabajo, y hacer cumplir las disposiciones emitidas por la SENRES.

6.8.2. Administración Financiera

A través de la administración financiera se administrará las rentas para financiar los gastos e inversiones municipales que contempla el presupuesto municipal. El presupuesto de la entidad, contendrá la programación anual de los ingresos por impuestos, tasas, contribuciones, rentas, transferencias, donaciones, y, los gastos corrientes y de capital, con sujeción a las normas y leyes del presupuesto. La Ley Orgánica de Administración Financiera y Control, las normas, principios y políticas de la contabilidad, serán base para los sistemas de tesorería y contabilidad municipal, Contabilidad registrará todas las obligaciones de patrimonio y de presupuestos; y Tesorería realizará la recepción, recaudación, depósito y entrega de recursos.

Alcanzará los fines que se persigue con el desarrollo de las siguientes funciones: dirección, supervisión, elaboración de catastros, emisión y control de títulos de crédito y formulación de datos estadísticos, contabilidad general, recaudación, pagos y bodegas. Así como se adquirirá los suministros, materiales y bienes muebles para distribuir a las dependencias municipales que requiere para su funcionamiento, como para administrar los inmuebles municipales. Este departamento tiene como unidades ejecutoras las siguientes dependencias: Dirección Financiera, Sección Rentas Municipales, Contabilidad, Tesorería, Bodega, y Recaudación.

6.8.3. Justicia, Policía y Vigilancia

Este programa tiene como finalidad cumplir y hacer cumplir de manera específica normas y disposiciones legales sobre la higiene, salubridad, ornato, obras públicas, uso de lugares y vías públicas, juegos, pesas y medidas, funcionamiento de ventas ambulantes, mercados, propaganda, uso de parques, avenidas, calles y jardines de

la ciudad, contenidas en leyes, ordenanzas y reglamentos municipales. Organizar y dirigir la administración de justicia dentro de la jurisdicción cantonal. Aplicar las normas correspondientes a los infractores y contraventores de las normas y disposiciones legales.

Investigar y esclarecer las infracciones cometidas dentro del ámbito municipal, coordinar con los organismos afines a sus funciones en el cumplimiento de actividades de beneficio y protección colectiva y cumplir con lo que establece la Ley Orgánica de Régimen Municipal, y el Orgánico Funcional de la Institución. Este departamento tiene como unidades ejecutoras las siguientes dependencias: Comisaría Municipal, Policía Municipal.

6.9. Servicios Comunales

6.9.1. Planificación Urbana y Rural

Al departamento de Planeamiento y Urbanismo le compete las funciones descritas y señaladas en la Ley Orgánica de Régimen Municipal, con el propósito fundamental de realizar la planificación del crecimiento urbano y rural del cantón, y que el crecimiento y desarrollo del cantón sea ordenado y la inversión sea de máximo rendimiento en beneficio de los barrios y sectores rurales del cantón, de la misma manera que conjuntamente con la unidad de avalúos y catastros, se encargarán de la actualización de los catastros urbano rurales. Este departamento tiene como unidades ejecutoras las siguientes dependencias: El director de este departamento estará a cargo de este programa con funciones de dirección, supervisión, ejecución, fiscalización y control en coordinación con los demás departamentos en especial y de manera directa con la Unidad de Avalúos y Catastros que pasa a formar parte de la Dirección de Planificación, conjuntamente con el Topógrafo del Municipio.

6.9.2. Higiene Ambiental: Unidad de Medio Ambiente y Turismo UMAT

Este programa tiene como propósito atender la higiene y salubridad del Cantón para lo cual realizará las siguientes actividades:

Reglamentación en lo relativo al manipuleo de alimentos, inspección de mercados, almacenes, mataderos, carnicerías, panaderías, bares, restaurantes, hoteles, pensiones y en general, los locales donde se fabriquen, guarden o expendan comestibles o bebidas de cualquier naturaleza, y velar porque en ellos se cumplan los procesos sanitarios.

Se vigilará y controlará la limpieza y recolección de basura de la ciudad, de sus calles, plazas, avenidas, parques, y su posterior depósito y clasificación en el relleno sanitario, con el personal técnico a cargo de la Jefatura de Higiene UGA, se planificará eventos de capacitación comunitaria, barriales, etc., tendientes a concienciar el manejo de los residuos sólidos, su clasificación y el cumplimiento de los horarios de recolección de los desechos. Este departamento tiene como unidades ejecutoras las siguientes dependencias: Higiene Ambiental, Subprogramas de Manejo Integral de Residuos sólidos, Servicios de Camales, y, Servicios de Mercados.

6.10. Otros Servicios Comunales

Este programa tiene como propósito el mantenimiento y construcción de obras a través de administración directa y por contrato para lo cual desarrollará las siguientes actividades:

- Construcción de obras programadas en el plan regulador municipal.
- Fiscalización y control de las obras en ejecución mediante contrato o concesión efectuada por la Ilustre Municipalidad.
- El mantenimiento de bienes inmuebles están a cargo de la Dirección de Obras Públicas Municipales, para lo cual utilizará el equipo motorizado de la Municipalidad, los trabajadores que se requieren para el mantenimiento de caminos y carreteras, edificios municipales, calles, plazas, parques, avenidas, etc.
- Además ejecutará las obras que interesen a las parroquias rurales, principalmente en cuanto se refiere a la construcción de caminos vecinales.

Este departamento tiene como unidad ejecutora a la: Dirección de Obras Públicas Municipales.

6.11. Servicios Económicos

6.11.1. Transportes y Vías

La Municipalidad por medio de este Programa, realizará el mantenimiento de las diferentes vías urbanas y de caminos vecinales del cantón utilizando los fondos del FONDVIAL DE LOJA y con la maquinaria de la Municipalidad, se la utiliza en el mantenimiento de los caminos vecinales, cuando se realizan las reparaciones con la ayuda de alguna asignación del Gobierno Central. Este departamento tiene como unidad ejecutora a la: Dirección de Obras Públicas Municipales.

6.12. Servicios Inclasificados

6.12.1. Gastos comunes de la Entidad y Servicio de la deuda

Este programa se encarga de atender todo lo relacionado a gastos comunes de la Entidad y servicio de la deuda por concepto de los préstamos concedidos por el Banco del Estado para:

- Mejoramiento y ampliación del sistema de agua potable de Cariamanga
- Construcción de la planta de tratamiento de agua potable
- Cubrir el desfinanciamiento del proyecto de ampliación y mejoramiento del sistema de agua potable de Cariamanga.
- Estudios definitivos de alcantarillado de la ciudad de Cariamanga.
- Electrificación rural de Calvas.
- Adquisición de equipo caminero.
- Obligaciones del 8vo contrato colectivo
- Obligaciones con el Patronato de Amparo Social

Además se considera el pago de la deuda flotante de diversos conceptos y Fondos ajenos conforme se adjunta en el presupuesto de gastos. Este departamento tiene como unidades ejecutoras a: El Alcalde del Concejo, Director Financiero, Contabilidad y Tesorería

7. EVALUACIÓN DEL OBJETO DE INVESTIGACIÓN

Hoy en día la seguridad de la información es un aspecto que influye notablemente en la protección de los activos de cualquier institución y que tiene como fin la protección de la información, uso, divulgación, interrupción o destrucción no autorizada, es decir proteger la confidencialidad, integridad y disponibilidad de la misma.

La implementación del sistema para la gestión de documentos utilizando certificados digitales en el Ilustre Municipio del cantón Calvas, cuenta con la factibilidad necesaria; puesto que es una institución que por el momento lleva a cabo este proceso en forma manual, lo cual influye en gran parte en que existan demoras en la entrega de documentación así como también que el contenido de cada documento sea conocido por terceras personas y por lo tanto no sea fiable. Para evitar aquello, y permitir que tanto el envío como la recepción de información sea eficiente, exista una mejor administración, y goce además de autenticidad se desarrolló el sistema antes mencionado, el cual se estipuló en el cumplimiento de los siguientes objetivos:

- Organizar los documentos de acuerdo a su índole de manera que se garantice eficiencia y eficacia durante su acceso.- La clasificación se encuentra establecida así: actas de sesiones, ordenanzas, resoluciones, convenios, órdenes de pago, solicitudes de los departamentos, boletines de prensa, oficios recibidos y enviados, procesos de contratación (contrataciones, licitaciones, calificaciones), contratos de obras ejecutadas, leyes y registros oficiales.
- Generar certificados de autenticación que permitan firmar digitalmente la información que se enviará y recibirá entre los diferentes departamentos que conforman la institución.- Proceso logrado a través del uso del algoritmo RSA, mismo que permite generar un par de claves: pública y privada, las cuales constituyen un certificado digital. Cabe indicar que el proceso de generación de claves es único, es decir dichas claves no se repetirán y se formarán además mediante la combinación de números primos elegidos aleatoriamente.
- Usar funciones hash para generar datos asociados (huella digital) basados en la encriptación asimétrica o codificación de los documentos digitales: Proceso logrado a través del uso del algoritmo MD5, el cual se encarga de generar un resumen del mensaje original con una longitud de 32 bits en formato hexadecimal; dicho resúmen será el que envíe al destinatario correspondiente, que además tiene como finalidad comprobar si un mensaje recibido es auténtico o fue adulterado.

- Aplicar claves privadas al documento original para obtener la firma digital que se enviará.- Las cuales tienen como finalidad permitir el envío de documentos firmados para garantizar de esta manera su confidencialidad y por supuesto seguridad.
- Auditar cada una de las acciones realizadas en los módulos del sistema; Proceso orientado a través de la generación de reportes con el propósito de tener un seguimiento más detallado de las acciones que realizan los usuarios en el sistema.
- Establecer e implantar niveles de seguridad y acceso en la aplicación que permitan el acceso únicamente a personal autorizado.- El acceso al sistema se encuentra restringido en base al rol al que se haya asignado a cada usuario al momento de su registro inicial en el sistema. Para ello se definió dos tipos de roles: Administrador y Usuario respectivamente.

  El rol de Administrador le pertenecerá a la persona encargada del funcionamiento de la aplicación, es decir será quien tendrá acceso a todos los módulos que conforman el sistema (Usuarios, Certificados, Categorías, Plantillas, Parámetros, Departamentos, Gestión de Documentos, Reportes y Respaldos); mientras que los usuarios comunes únicamente tendrán acceso al módulo de Gestión de Documentos.

8. DESARROLLO DE LA PROPUESTA ALTERNATIVA

8.1. DESCRIPCIÓN DEL PROBLEMA

Dentro de cualquier organización la información fluye día con día, y cada actividad genera más información que puede apoyar las distintas tareas que se llevan a cabo para su buen funcionamiento.

La información es calificada como uno de los factores más influyentes que dirigen el rumbo de cualquier organización; Por ello es recomendable dejar de lado el uso de técnicas de gestión tradicionales en el ámbito administrativo, ya que esto, ocasiona inconvenientes como: retrasos en la entrega de información, pérdida de tiempo en la búsqueda de algún documento, confusiones, desorganización y demás incidentes que pueden afectar el cumplimiento de actividades dentro de las instituciones.

El Ilustre Municipio del cantón Calvas es una institución que se encuentra inmersa dentro de éstos aspectos, ya que por tener un gran volumen de información requiere su automatización, esto con la finalidad de que al momento de acceder a la misma se facilite su búsqueda, envío y recepción según sea la necesidad. Actualmente se presentan inconvenientes durante el envío y recepción de datos entre los diferentes departamentos ya que por ser una acción manual que se efectúa mediante boletines de aviso o en forma directa hacia el resto del personal requiere demasiado tiempo para ser accedida por su destinatario, además de tener el inconveniente de que su contenido sea conocido por el resto de personas, así como también producir demoras para conocer el resultado de un trámite que se efectúo o se está efectuando. Todo ello ocasiona que exista un servicio de baja calidad además de inseguro en lo que a información se refiere en la institución.

Actualmente los documentos que se tramitan son: Actas de sesiones, ordenanzas, resoluciones, convenios, órdenes de pago, solicitudes de los departamentos, boletines de prensa, oficios recibidos y enviados, procesos de contratación (contrataciones, licitaciones, calificaciones), contratos de obras ejecutadas, leyes y registros oficiales. En lo que se refiere a documentos con mayor demanda constan las solicitudes de compra, ventas, peticiones de los demás departamentos y ciudadanía en general.

El envío de documentos tiene lugar considerando los siguientes departamentos: Obras Públicas, Financiero, Planificación, Tesorería, Secretaria, y Procurador Síndico. Así mismo, existen otras dependencias, que tienen relación directa con los departamentos

mencionados anteriormente: Rentas, Comisaría, Contabilidad, Avalúos y Catastros, Biblioteca, Sistemas, Unidad de Gestión Ambiental, Proveeduría y Guardalmacén.

El optar por la implementación de un sistema para automatizar los servicios antes mencionados permitirá garantizar autenticidad, confidencialidad y seguridad en la información.

8.2. DESCRIPCIÓN GENERAL DEL SISTEMA

La fácil disponibilidad que poseen las computadoras y las tecnologías de información en general, han creado una revolución informática en la sociedad y de forma particular en la mayoría de instituciones. El manejo de información generada por computadora difiere en forma significativa del manejo de datos producidos manualmente. Por éstas razones es que ha resultado conveniente el desarrollo un sistema destinado a la automatización de documentos que se tramitan en el Municipio de Calvas, utilizando certificados digitales como una opción para resguardar los datos de manera segura e íntegra al momento de su creación, acceso y traslado.

Dicho sistema está basado en algoritmos de encriptación asimétrica (RSA) que consisten en convertir un texto legible en otro ilegible, es decir los documentos se codifican y solo pueden ser leídos si se dispone de la clave que ha sido asignada para llevar a cabo su tramitación. Cada usuario para tal efecto dispondrá de un par de claves: pública y privada que constan en su certificado digital que haya sido asignado.

El proceso de verificación de un documento tiene lugar al generar un hash del documento que se recibió, dicho resumen se origina a partir del documento original, haciendo uso para ello del algoritmo MD5. Al momento en que un usuario recibe un documento firmado se generará un hash, el cual será comparado con el hash recibido, si los dos resultado son idénticos el documento es auténtico y no tiene ninguna alteración desde su envío. Para cumplir con estos procesos de envío y recepción de documentos entre los diferentes departamentos de la institución, se estructuró el sistema en módulos, los cuales están destinados a cumplir con una función determinada, así:

Orden	Nombre del Módulo	Función	Responsable
1	**Sistema**	Verificar el inicio o finalización de la sesión que cada usuario ha tenido en el sistema.	*Administrador/ Usuario*
2	**Usuario**	Permitir la creación, búsqueda, edición, y eliminación de usuarios. Solo los usuarios registrados tendrán acceso al sistema, mediante su nombre de usuario y contraseña la cual será asignada por parte del administrador.	*Administrador*
3	**Certificado**	Crear o dar de baja al certificado activo de un usuario determinado. El certificado será dado de baja por condiciones como; acceso no autorizado a la clave privada del usuario, pérdida y ausencia prolongada del usuario en la institución.	*Administrador*
4	**Categoría**	Permitir la creación, edición y eliminación de categorías a las que los diferentes documentos pertenecen. Cada categoría dispondrá de una referencia que actúa como un identificativo durante el envío y recepción de la información.	*Administrador*
5	**Departamento**	Permitir la creación, edición y eliminación de departamentos establecidos por la institución.	*Administrador*
6	**Plantilla**	Permitir definir la estructura de un documento, en lo que a encabezado y pie de página se refiere.	*Administrador*
7	**Parámetro**	Permitir que la aplicación sea configurada y adaptada a otras instituciones con similares requerimientos. Para ello definimos parámetros básicos que pueden ser editados.	*Administrador*
8	**Documento**	Permitir la creación, edición, eliminación, envío, almacenamiento y recepción de documentos que pueden o no estar firmados.	*Administrador /Usuario*
9	**Reporte**	Permitir visualizar reportes generados a partir de las acciones efectuadas en el sistema por parte de los usuarios que han iniciado sesión. De igual manera	*Administrador*

		este módulo será capaz de generar archivos log's como una alternativa más detallada para seguimiento de la aplicación	
10	**Respaldo**	Permitir respaldar toda la información del sistema (Base de Datos (Ver Anexo 2) archivos subidos, archivos de imagen) en caso de pérdida de datos y evitar con ello retrasos en la entrega y envío de documentación. Los respaldos serán automáticos y manuales; además existirán las opciones de restaurar y eliminar un respaldo. Los respaldos que se generan se almacenarán en una carpeta destino que se haya elegido en el Servidor; la cual a su vez contiene las carpetas de imagen, archivos subidos y el script de la base de datos	*Administrador*

Tabla 6. Estructura de Módulos del SGD-GADCC

8.3. REQUERIMIENTOS FUNCIONALES

Entre los requerimientos funcionales que el sistema debe cumplir están el permitir:

CÓDIGO	DESCRIPCIÓN	CATEGORÍA
RF01	Logear usuarios (iniciar sesión, cerrar sesión)	Evidente
RF02	Visualizar los usuarios que han iniciado sesión	Evidente
RF03	Administrar usuarios(crear, buscar, editar, eliminar)	Evidente
RF04	Restringir el acceso a las funcionalidades del sistema	Evidente
RF05	Cambiar contraseña de seguridad	Evidente
RF06	Administrar certificados (generar nuevo, dar de baja)	Evidente
RF07	Controlar la creación y expiración de los certificados.	Oculto
RF08	Generar claves públicas y privadas con el algoritmo RSA.	Evidente
RF09	Validar claves que se hayan asignado a los usuarios.	Oculto

RF10	Guardar claves en dispositivos de almacenamiento.	Evidente
RF11	Administrar categorías(crear, editar, eliminar)	Evidente
RF12	Administrar plantillas (crear, editar, eliminar)	Evidente
RF13	Administrar departamentos (crear, editar, eliminar)	Evidente
RF14	Editar parámetros	Evidente
RF15	Crear/ enviar documentos	Evidente
RF16	Buscar documentos	Evidente
RF17	Revisar documentos de la bandeja de entrada, salida, eliminados y borradores.	Evidente
RF18	Agregar, eliminar y buscar contactos	Evidente
RF19	Crear, editar y eliminar borradores	Evidente
RF20	Adjuntar información o archivos.	Evidente
RF21	Descargar archivos o documentación recibida.	Evidente
RF22	Reenviar archivos o documentación recibida.	Evidente
RF23	Encriptar y desencriptar información con el algoritmo RSA.	Oculto
RF24	Obtener hash del mensaje.	Evidente y oculto
RF25	Comprobar autenticidad de la información recibida.	Oculto
RF26	Generar ruta del documento que se recibe.	Evidente
RF27	Eliminar documentos recibidos	Evidente
RF28	Generar reportes de las acciones efectuadas en los módulos del sistema.	Evidente
RF29	Visualizar reportes en formato .pdf	Evidente
RF30	Auditar las acciones realizadas en el sistema	Evidente
RF31	Generar archivos log's para el seguimiento de la aplicación.	Evidente y oculto
RF32	Administrar respaldos del sistema	Evidente y oculto

Tabla 7. Requerimientos Funcionales

8.4. REQUERIMIENTOS NO FUNCIONALES

Entre los requerimientos no funcionales, definimos los que a continuación se detallan:

CÓDIGO	DESCRIPCIÓN
RNF01	El sistema deberá contar con una interfaz gráfica interactiva, amigable en entorno web
RNF02	Deberá ser construido en Lenguaje de programación JAVA, con el entorno de programación JSF
RNF03	Funcionará con el Servidor Apache Tomcat 6.0.14 o superior
RNF04	Utilizará como navegador a Mozilla (recomendado)
RNF05	La información será administrada en una Base Datos MySql v5 o superior
RNF06	Formato de documentación estandarizado, que permita realizar actualizaciones y operaciones de mantenimiento a la información de manera fácil y sencilla
RNF07	El sistema será multiusuario.
RNF08	Se basará en la arquitectura Modelo Vista Controlador de Casos de Uso, el cual facilitará dar la funcionalidad a la interfaz gráfica de usuario
RNF09	El sistema deberá trabajar con la hora y fecha actualizadas del sistema.

Tabla 8. Requerimientos No Funcionales

8.5. DEFINICIÓN DE ACTORES Y METAS

IDENTIFICACIÓN DE CASOS DE USO

ACTOR	META	CÓDIGO	CASO DE USO	CÓDIGO
Administrador/ Usuario	Iniciar Sesión	MT01	Logear Usuarios	CU01
	Cerrar Sesión	MT02		
Administrador	Crear Usuario	MT03	Administrar Usuarios	CU02
	Buscar Usuario	MT04		
	Editar Usuario	MT05		
	Cambiar Clave	MT06		
	Eliminar Usuario	MT07		
	Editar Perfil	MT08		
	Crear Certificado	MT09	Administrar Certificados	CU03
	Dar de Baja Certificado	MT10		
	Crear Categoría	MT11	Administrar Categorías	CU04
	Editar Categoría	MT12		
	Eliminar Categoría	MT13		
	Crear Plantilla	MT14	Administrar Plantillas	CU05
	Editar Plantilla	MT15		
	Eliminar Plantilla	MT16		
Administrador	Crear Departamento	MT17	Administrar Departamentos	CU06
	Editar Departamento	MT18		
	Eliminar Departamento	MT19		
Administrador	Editar Parámetros	MT20	Administrar Parámetros	CU07
Usuario/ Administrador	Crear/Enviar Documentos	MT21	Gestionar Documentos Electrónicos	CU08
Sistema	Encriptar con RSA	MT22		
Usuario/ Administrador	Buscar Contacto	MT23		
	Agregar Contacto	MT24		
	Eliminar Contacto	MT25		
	Leer Documentos Recibidos	MT26		
	Eliminar Bandeja de Entrada.	MT27		
	Crear un Borrador	MT28		
	Editar un Borrador	MT29		

	Eliminar un Borrador	MT30	Gestionar Documentos Electrónicos	CU08
	Presentar Documentos	MT31		
Administrador	Buscar Documentos	MT32		
	Generar Reportes	MT33	Generar Reportes	CU09
	Ver Archivos Log's	MT34		
	Auditar Logeo	MT35	Efectuar Auditoria	CU10
	Auditar Creación de Usuario	MT36		
	Auditar Edición de Usuario	MT37		
	Auditar Eliminación de Usuario	MT38		
	Auditar Creación de Certificado	MT39		
	Auditar Actualización de Certificado	MT40		
	Auditar Creación de Categoría.	MT41		
	Auditar Edición de Categoría.	MT42		
	Auditar Eliminación de Categoría.	MT43		
	Auditar Creación de Plantilla	MT44		
	Auditar Edición de Plantilla	MT45		
	Auditar Eliminación de Plantilla	MT46		
	Auditar Creación de Departamento	MT47		
	Auditar Edición de Departamento	MT48		
	Auditar Eliminación de Departamento.	MT49		
	Auditar Edición de Parámetro.	MT50		
	Auditar Creación de Documento	MT51		
	Auditar Eliminación de Documento.	MT52		
	Generar Archivos Log's	MT53		

Administrador	Buscar Respaldo	MT54	Administrar Respaldos	CU11
	Crear Respaldo	MT55		
	Restaurar Respaldo	MT56		
	Eliminar Respaldo	MT57		

Tabla 9. Identificación de Casos de Uso

8.6. MODELO DE CASOS DE USO

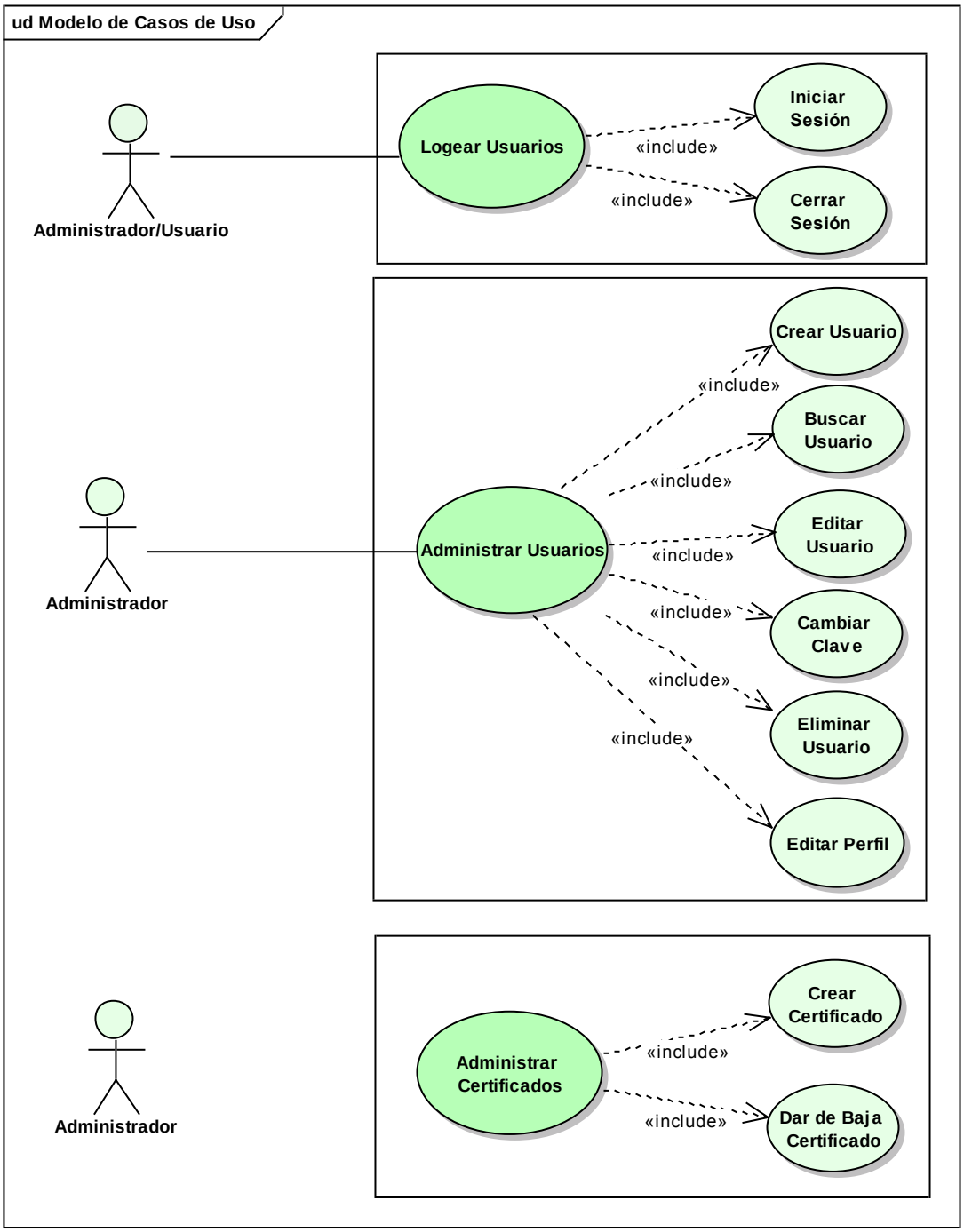


Fig. 10. Identificación de Casos de Uso I

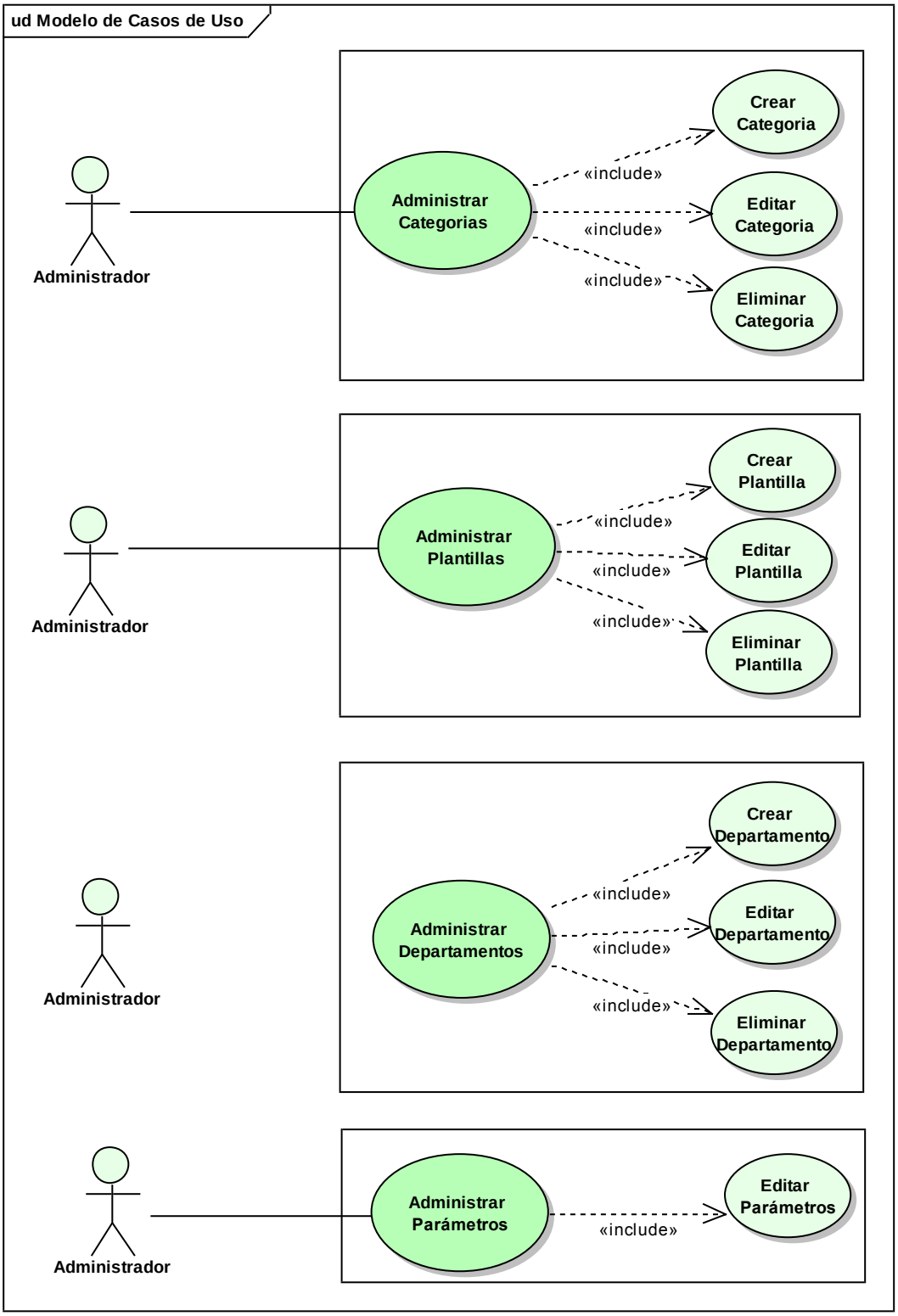


Fig. 11. Identificación de Casos de Uso II

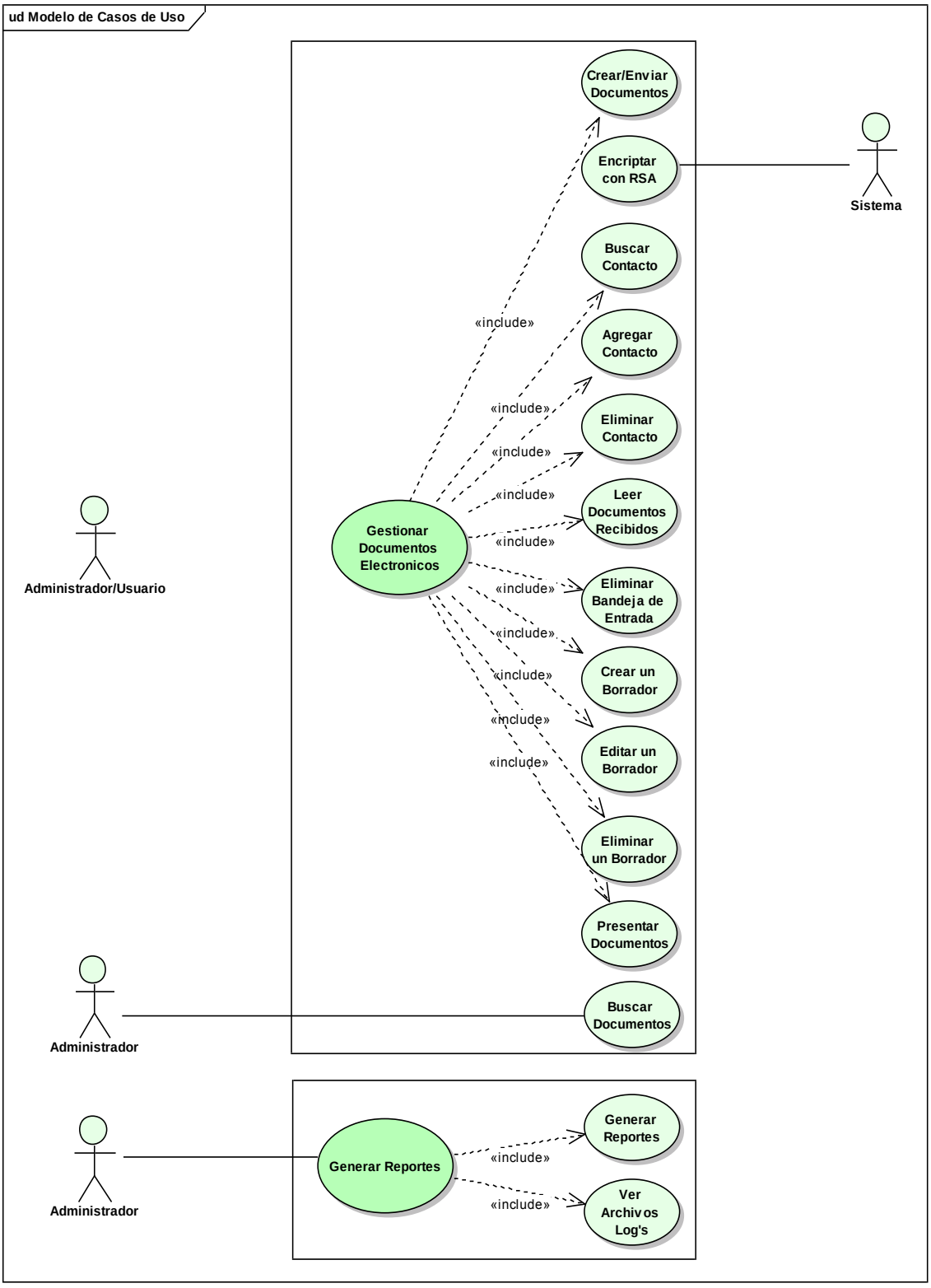


Fig. 12. Identificación de Casos de Uso III

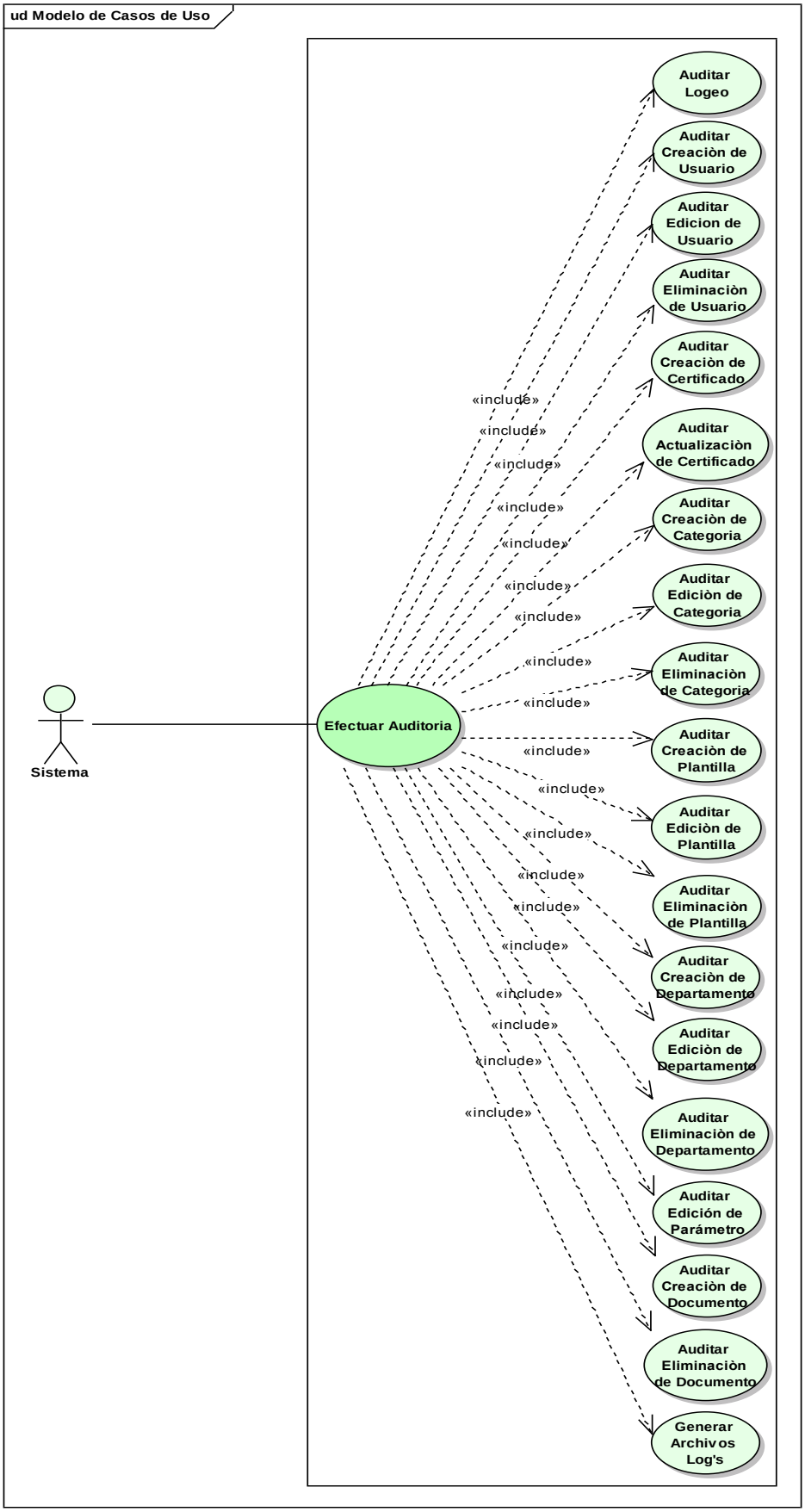


Fig. 13. Identificación de Casos de Uso IV

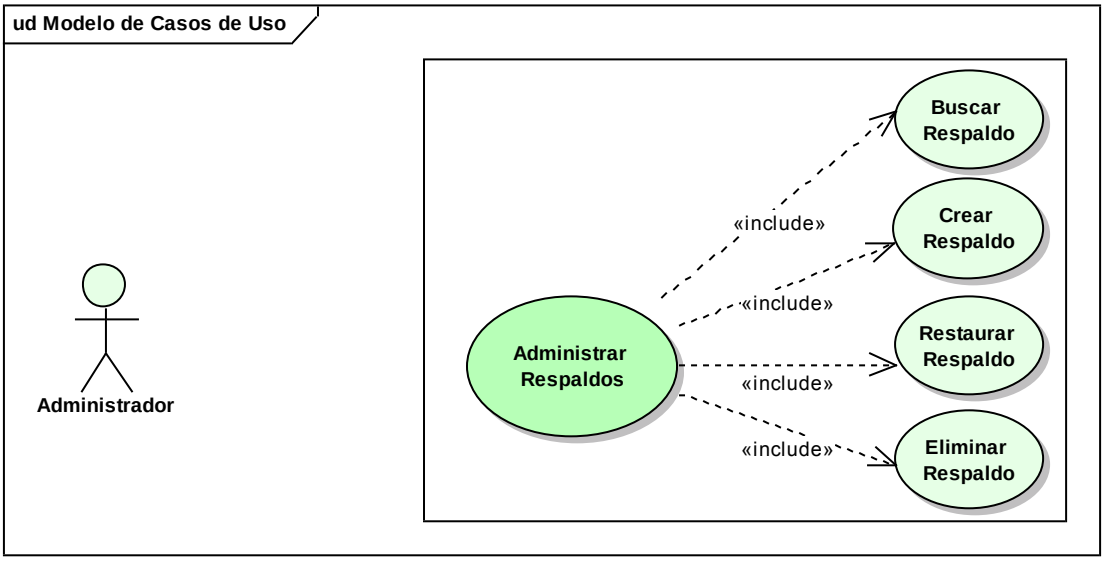


Fig. 14. Identificación de Casos de Uso V

8.7. PROTOTIPADO DE PANTALLAS

Pag01: Bienvenida

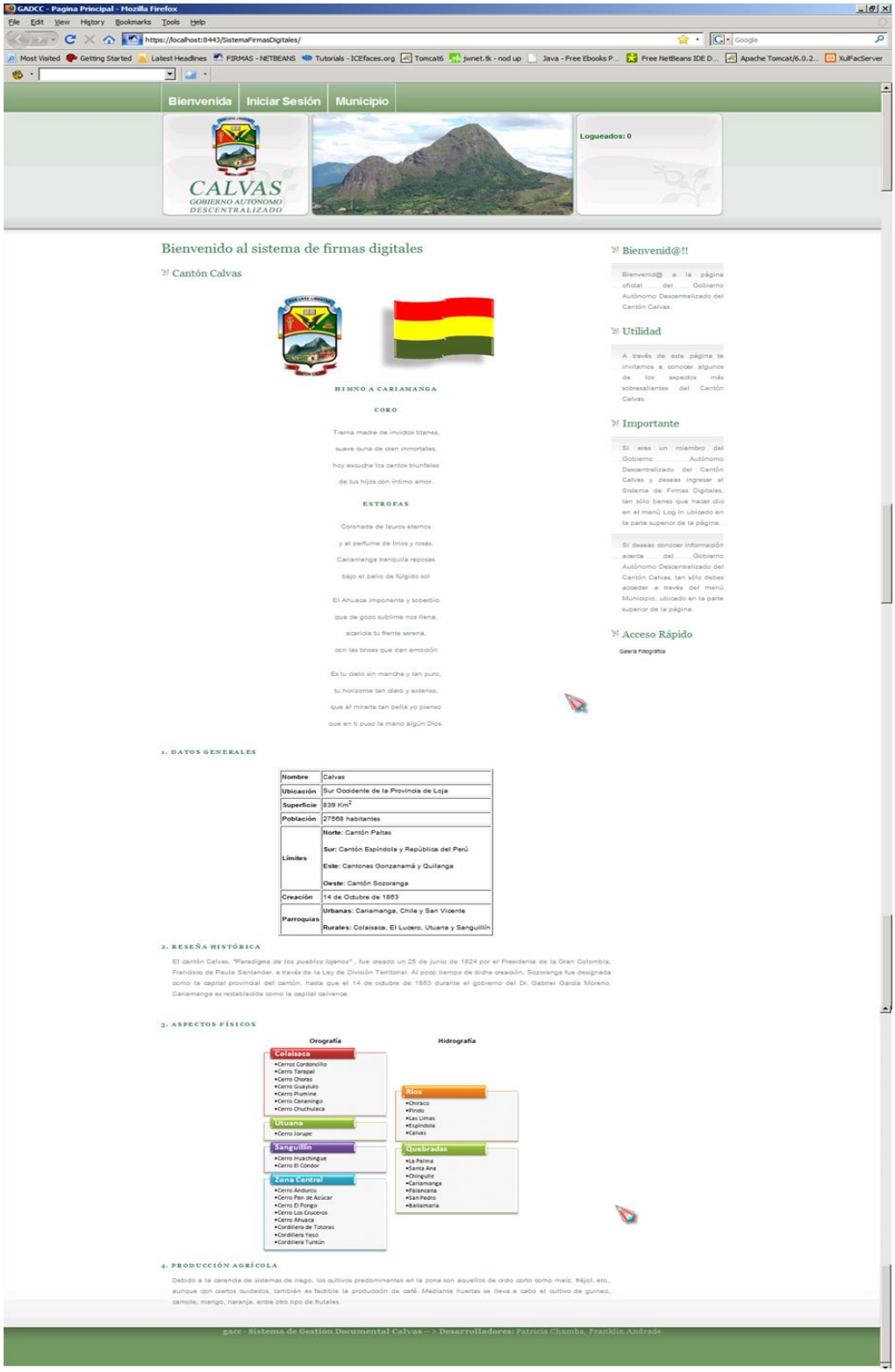


Fig. 15. Bienvenida

Pag02: IniciarSesión

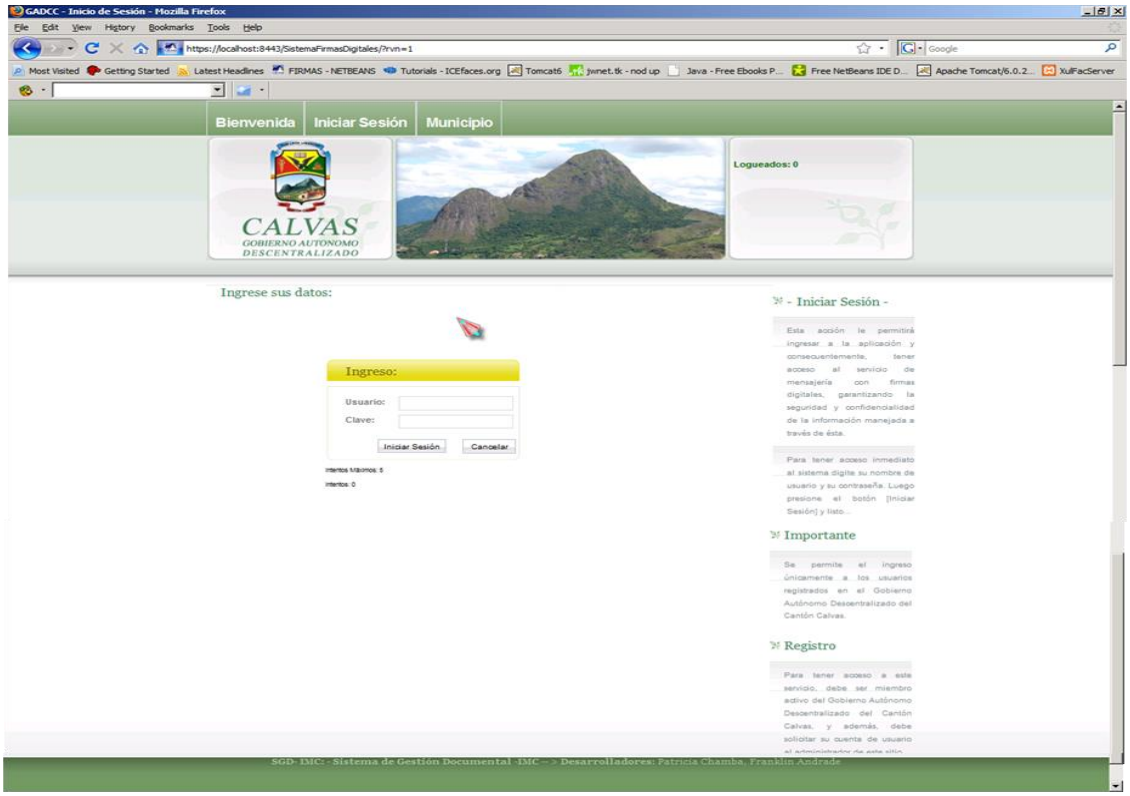


Fig. 16. Iniciar Sesión

Pag03: Inicio

Fig. 17. Inicio

Pag04: ErrorIniciarSesión

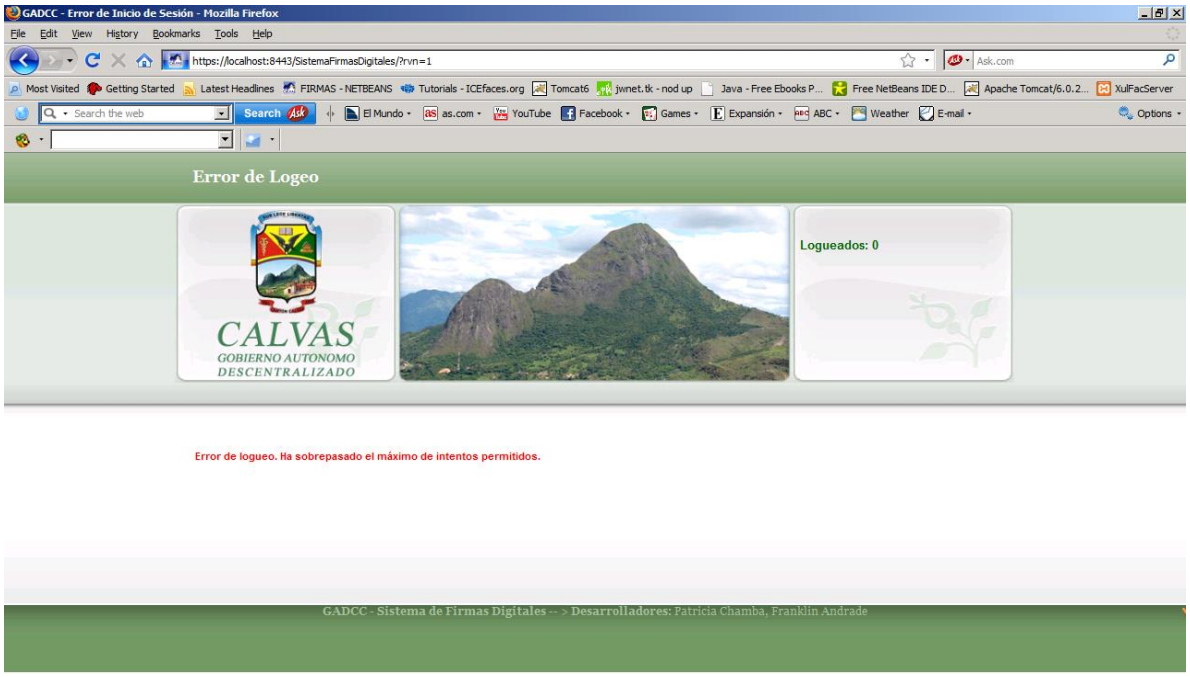


Fig. 18. Error al Iniciar Sesión

Pag05: AdministrarUsuarios

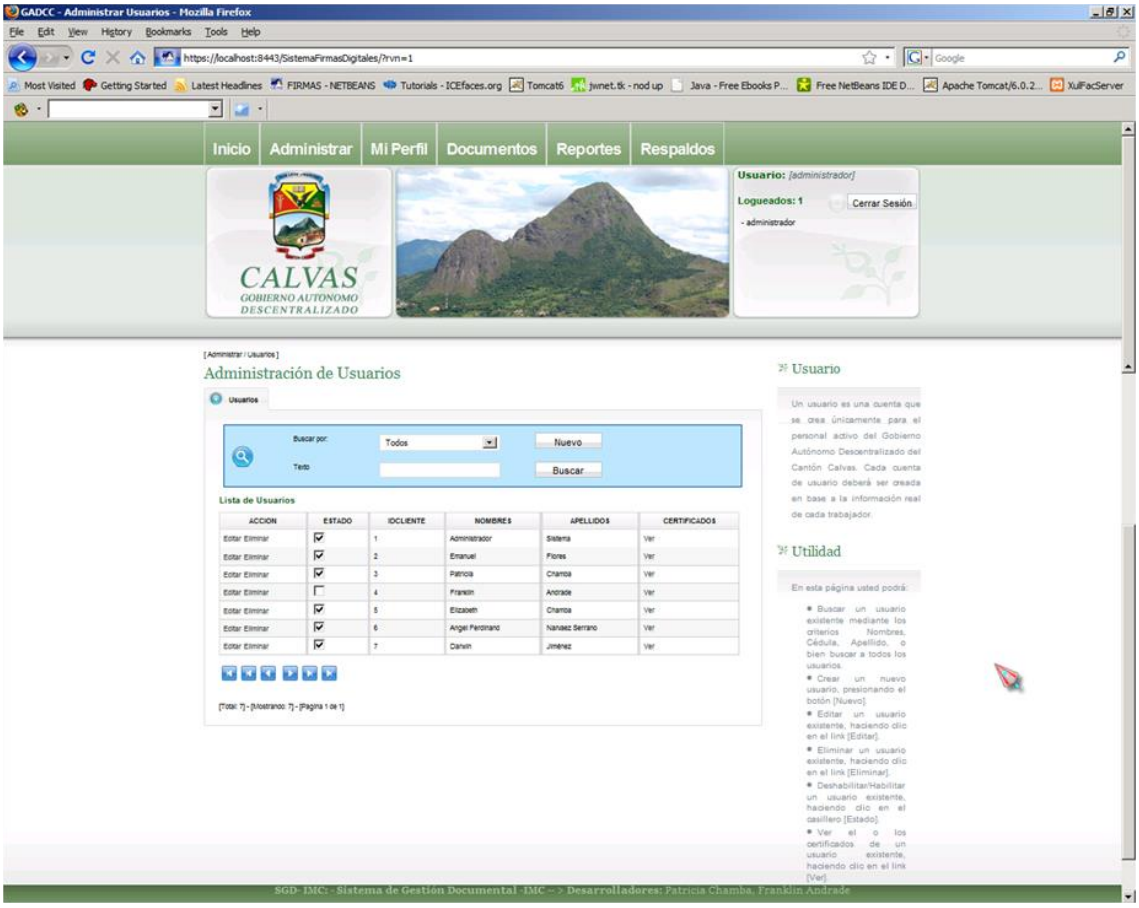


Fig. 19. Administrar Usuarios

Mensaje de confirmación [Eliminar Usuario]

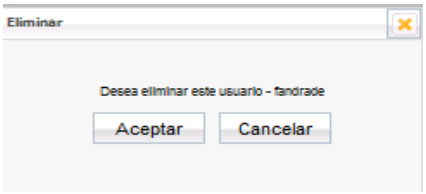


Fig. 20. Eliminar Usuario

Mensaje de aviso [Integridad Referencial]

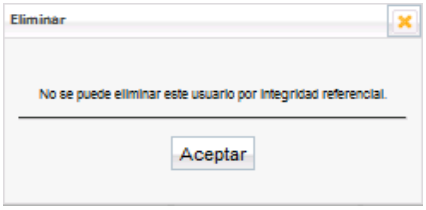


Fig. 21. Integridad Referencial Usuario

Pag06: EditarUsuario

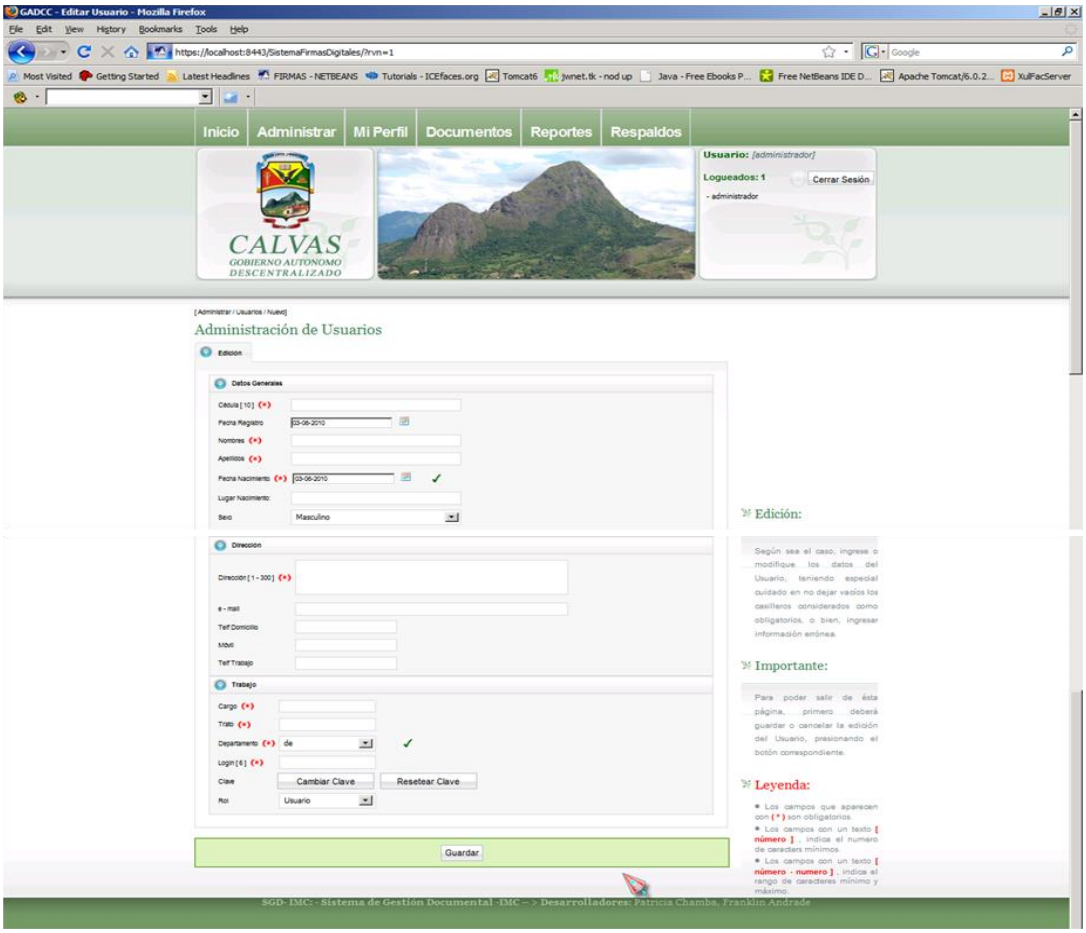


Fig. 22. Editar Usuario

Diálogo [Cambiar Clave]

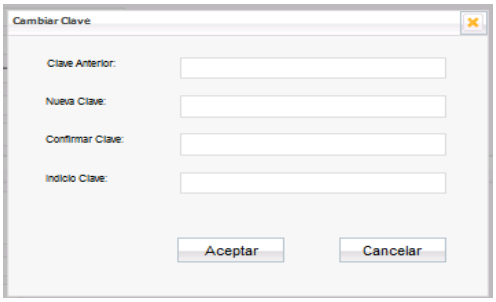


Fig. 23. Cambiar Clave

Pag07: Certificados

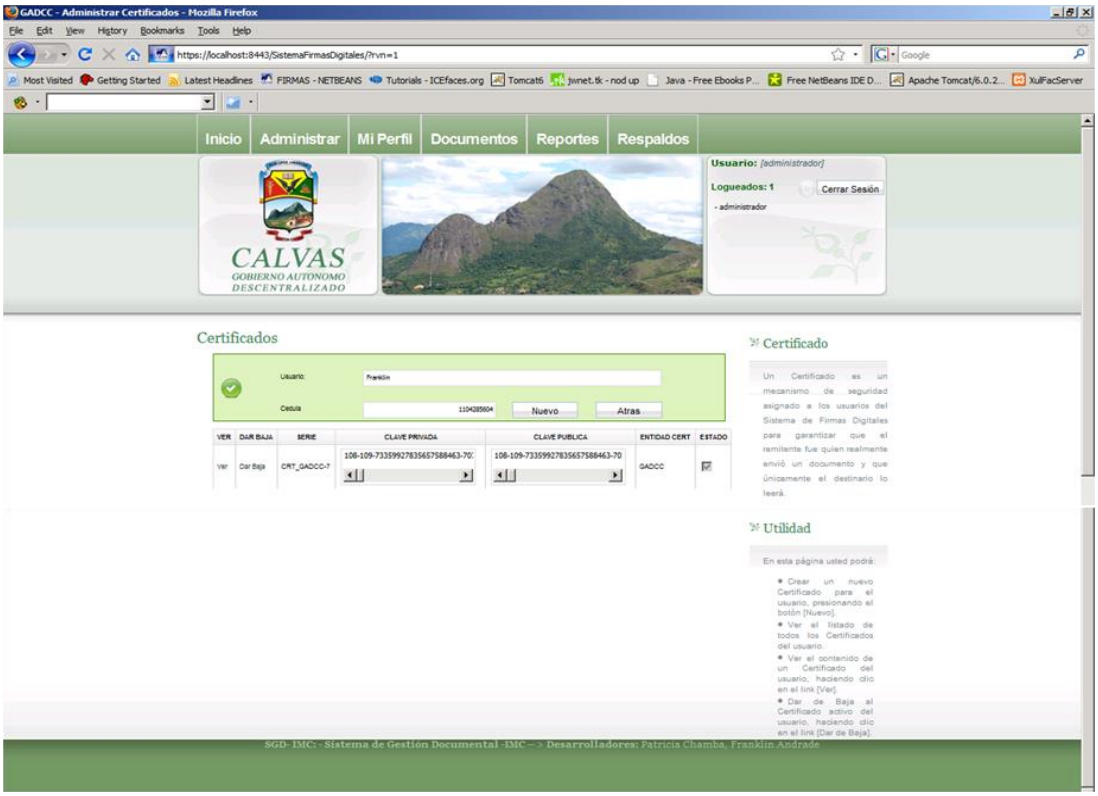


Fig. 24. Certificados

Diálogo [Confirmar Baja]

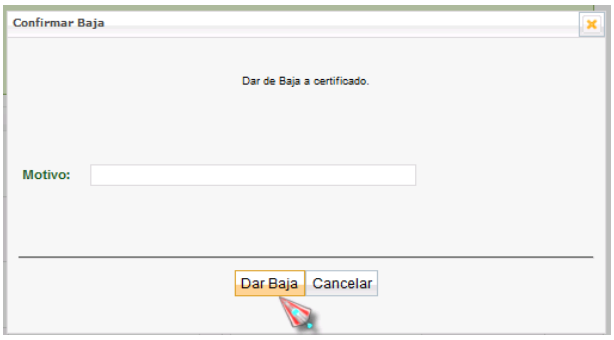


Fig. 25. Confirmar Baja

Mensaje de aviso [Usuario dispone de un certificado activo]

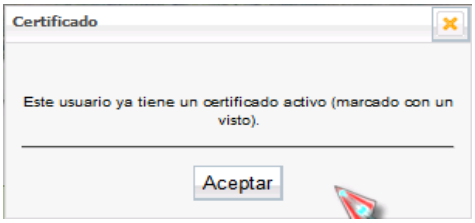


Fig. 26. Usuario con Certificado Activo

Pag08: EditarCertificado

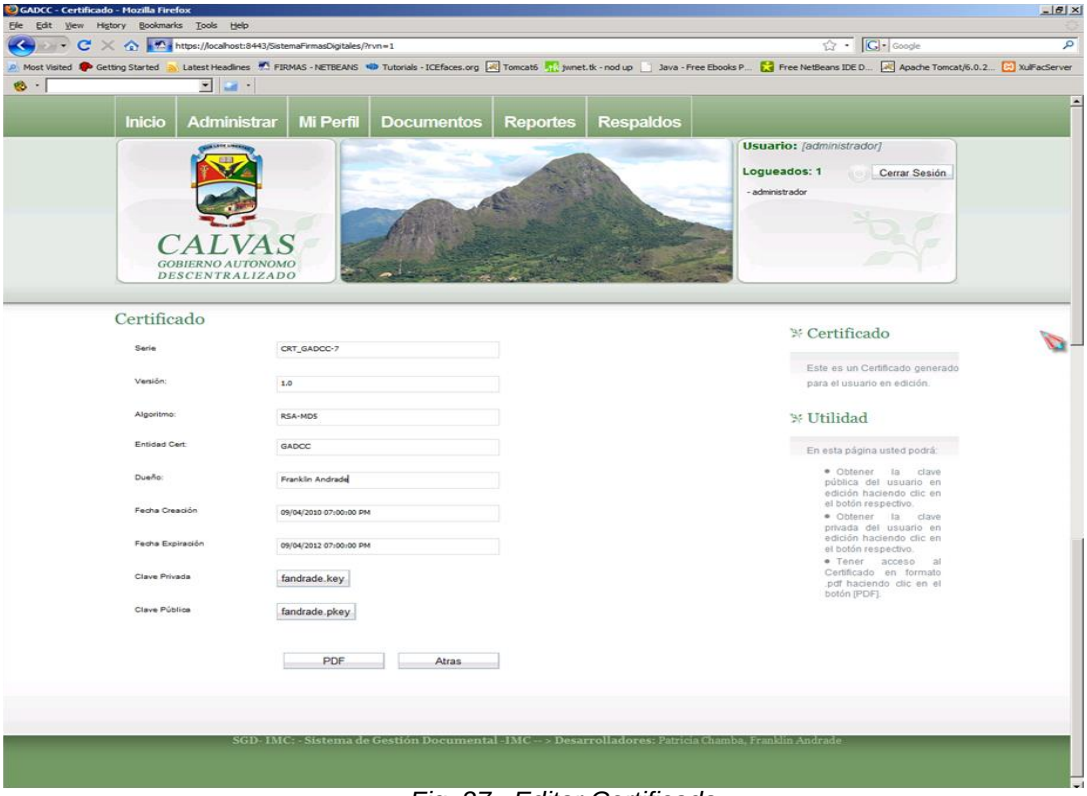


Fig. 27. Editar Certificado

Asistente para descargar clave privada

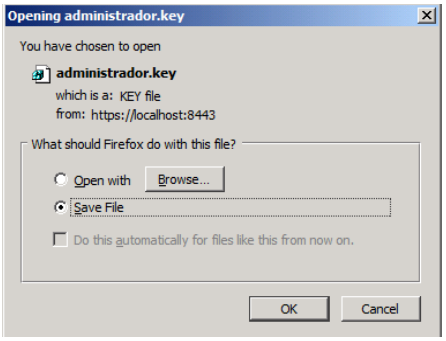


Fig. 28. Descargar Clave Privada

Asistente para descargar clave pública

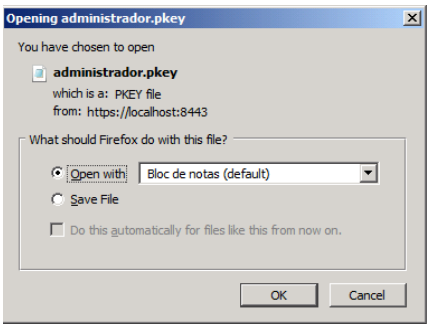


Fig. 29. Descargar Clave Pública

Certificado PDF

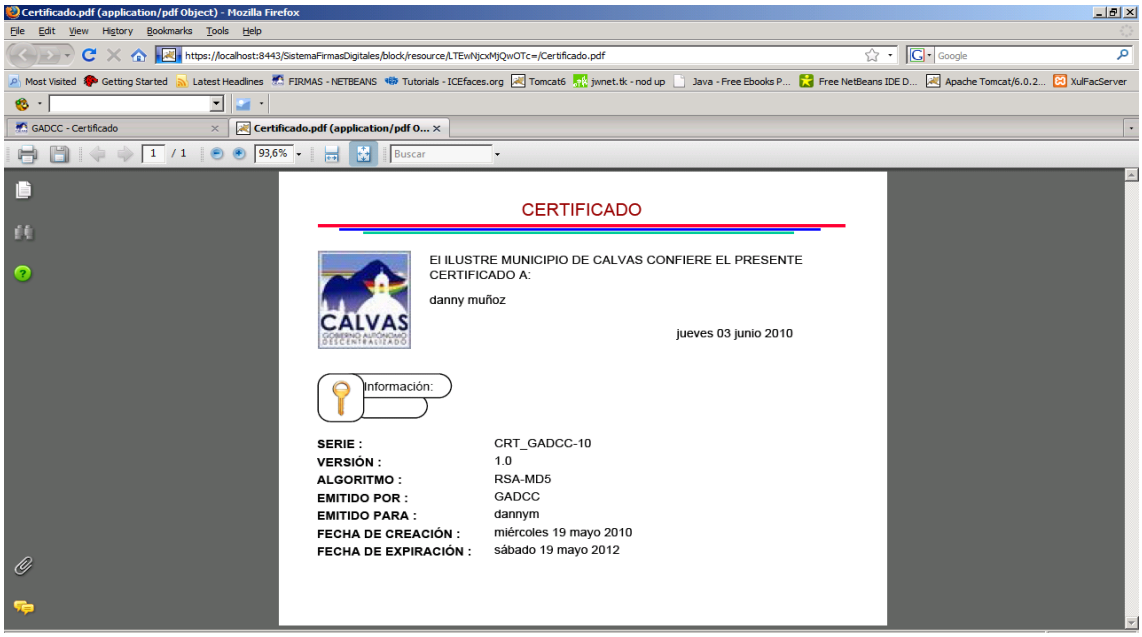


Fig. 30. Certificado PDF

Pag09: MiPerfil

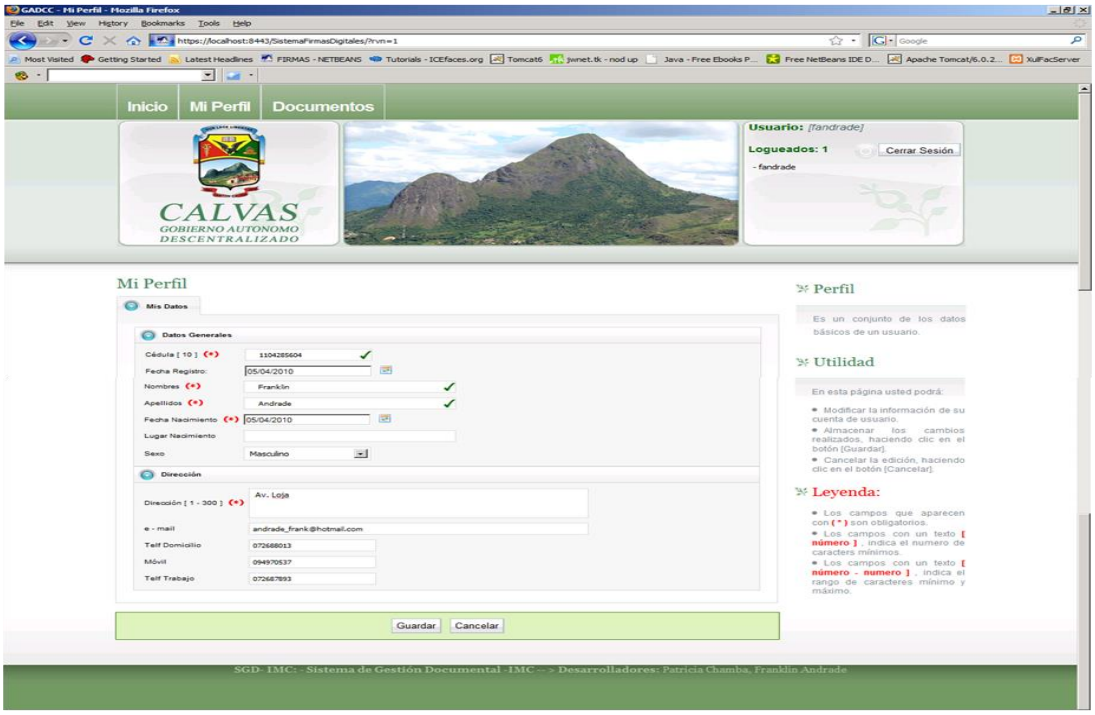


Fig. 31. Mi Perfil

Pag10: AdministrarCategorías

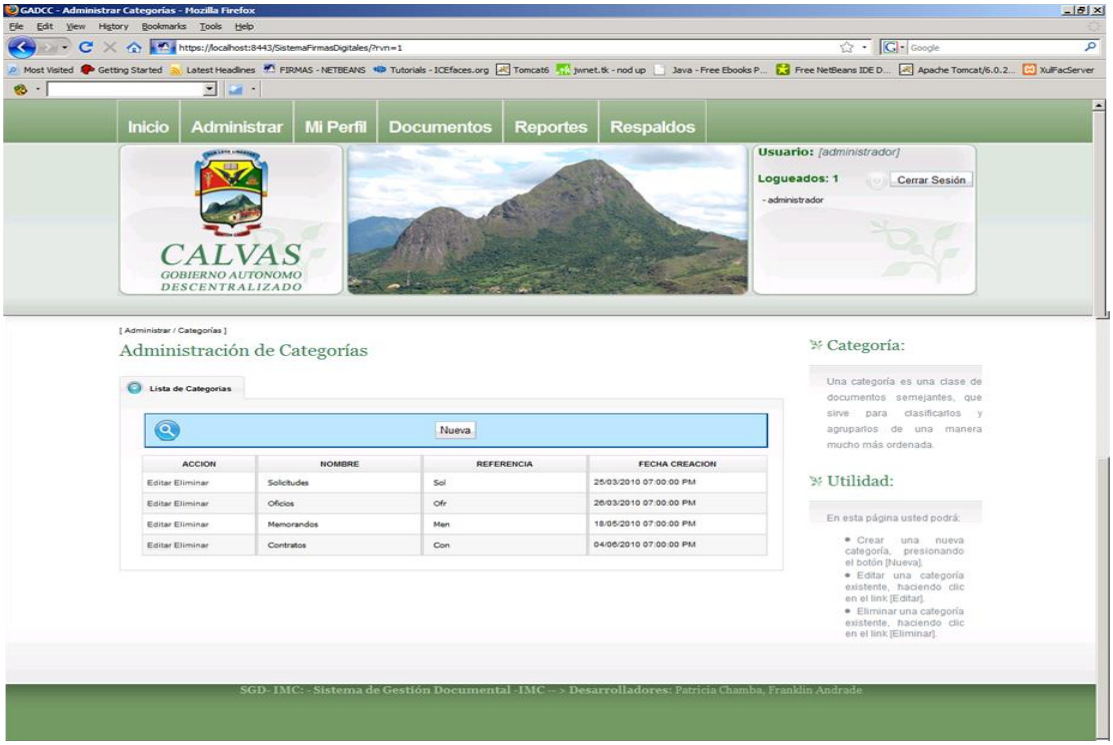


Fig. 32. Administrar Categorías

Mensaje de confirmación [Eliminar Categoría]

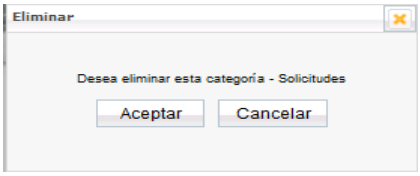


Fig. 33. Eliminar Categoría

Mensaje de aviso [Integridad Referencial]

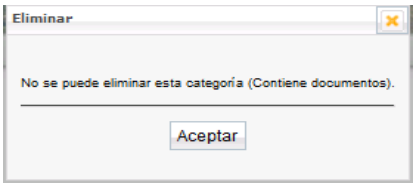


Fig. 34. Integridad Referencial Categoría

Pag11: EditarCategoría

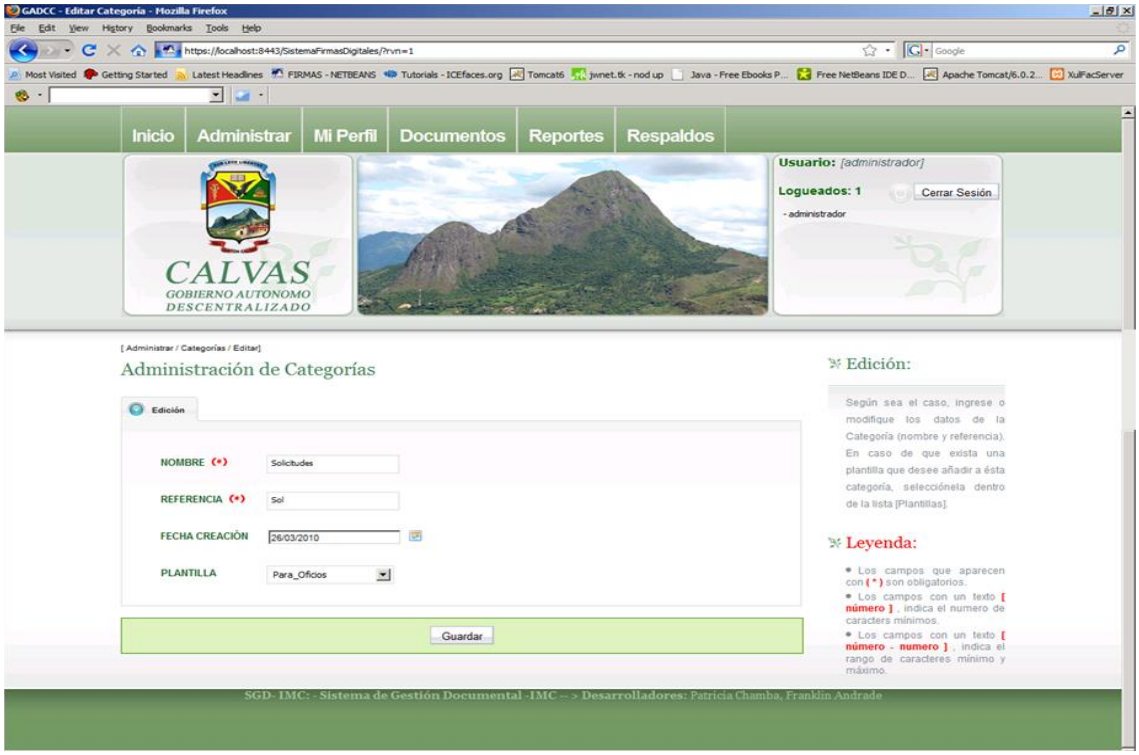


Fig. 35. Editar Categoría

Pag12: AdministrarPlantillas

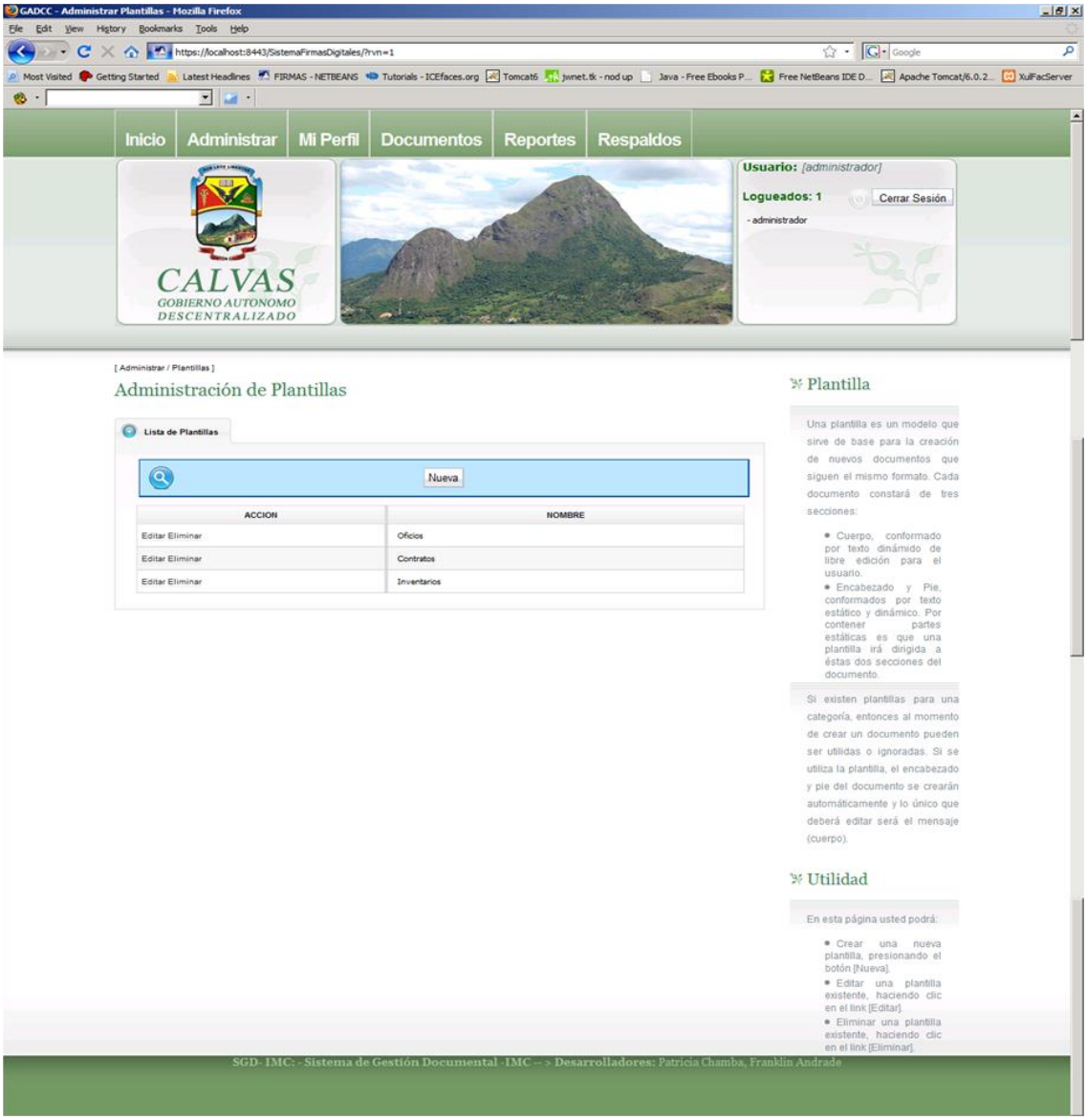


Fig. 36. Administrar Plantillas

Mensaje de confirmación [Eliminar Plantilla]

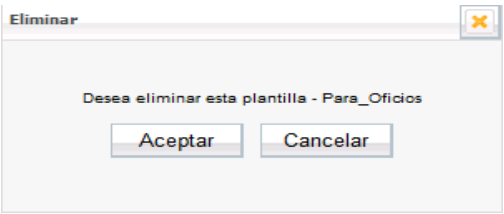


Fig. 37. Eliminar Plantilla

Pag13: EditarPlantilla

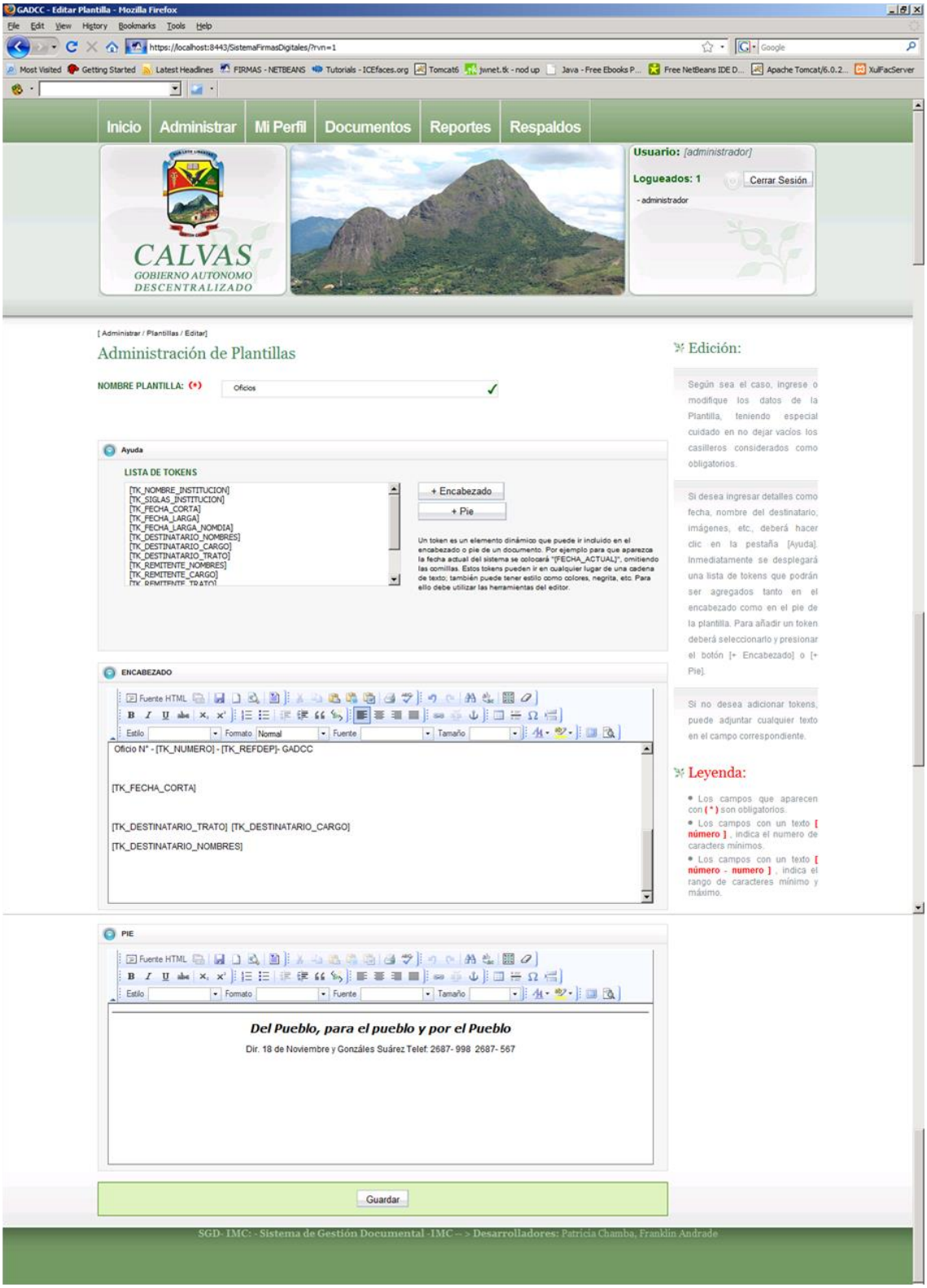


Fig. 38. Editar Plantilla

Pag14: AdministrarDepartamentos

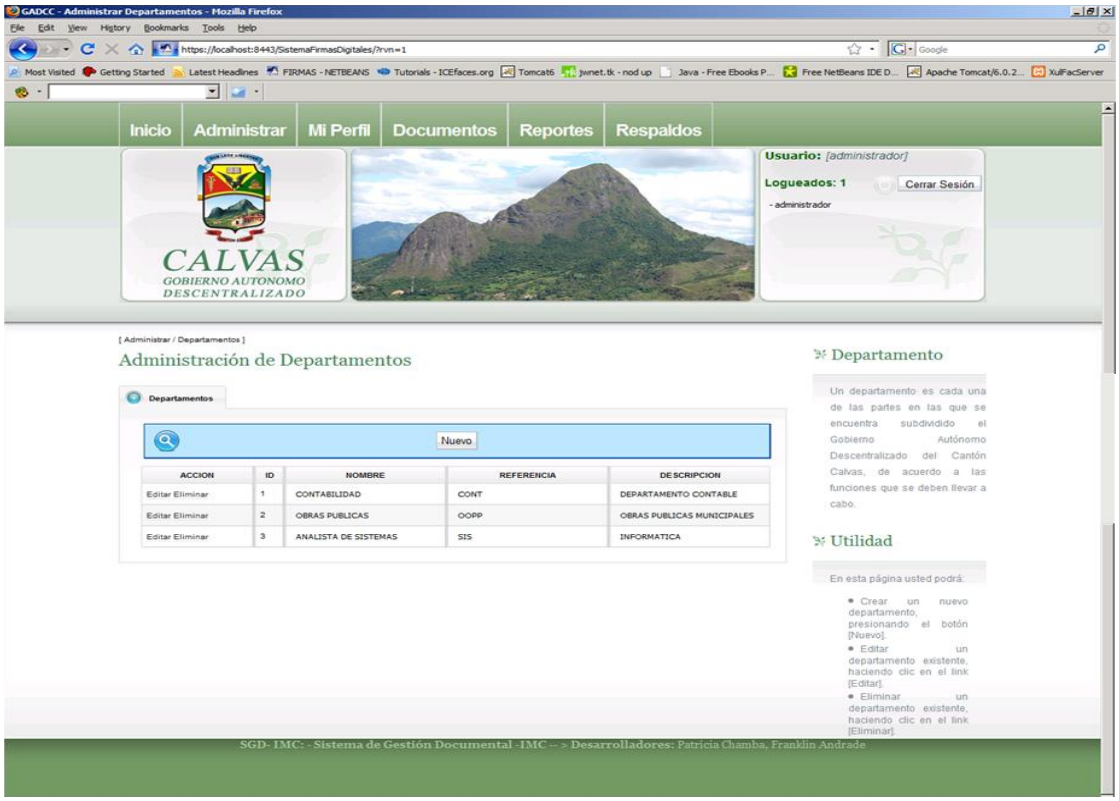


Fig. 39. Administrar Departamentos

Mensaje de confirmación [Eliminar Departamento]

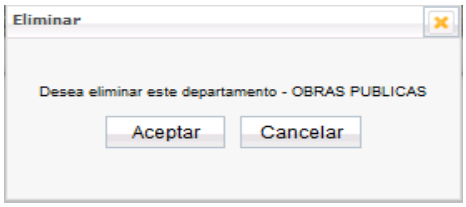


Fig.40. Eliminar Departamento

Mensaje de aviso [Integridad Referencial]

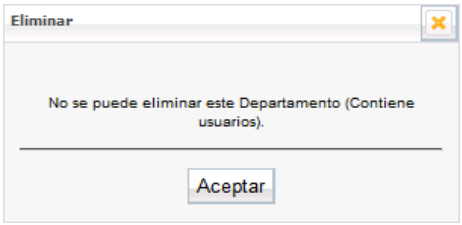


Fig. 41. Integridad Referencial Departamento

Pag15: EditarDepartamento

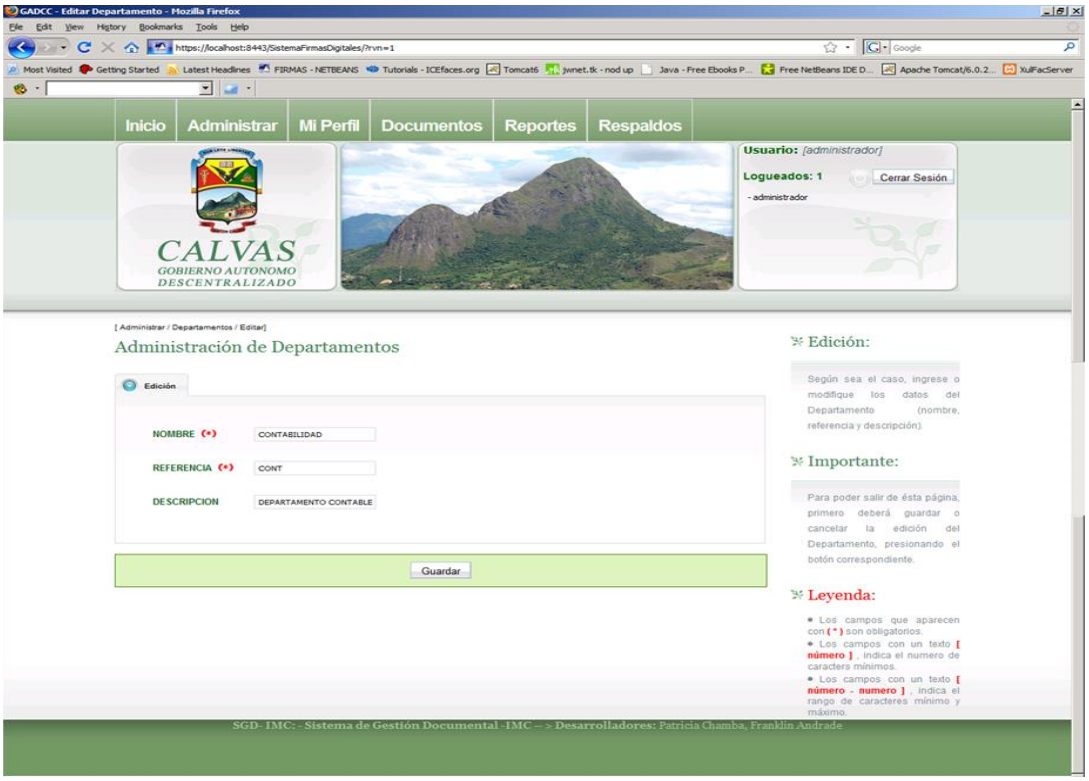


Fig. 42. Editar Departamento

Pag16: AdministrarParámetros

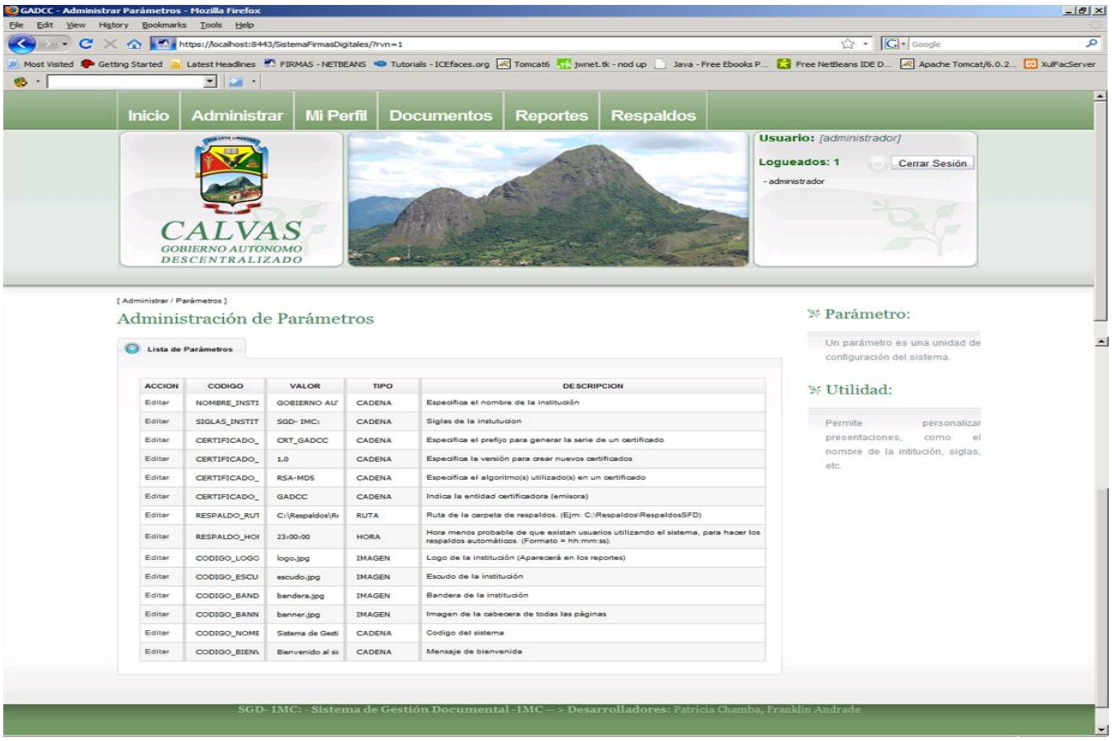


Fig. 43. Administrar Parámetros

Pag17: EditarParámetro

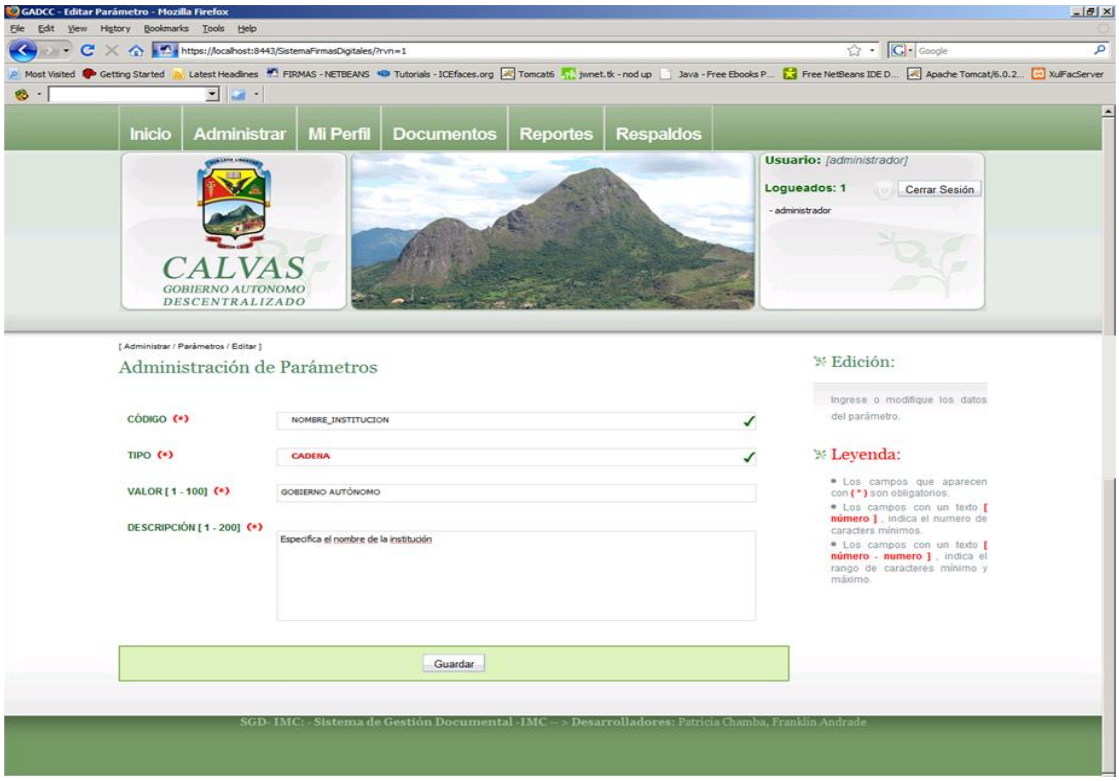


Fig. 44. Editar Parámetro

Pag18: AdministrarDocumentos/sección Bandeja de entrada

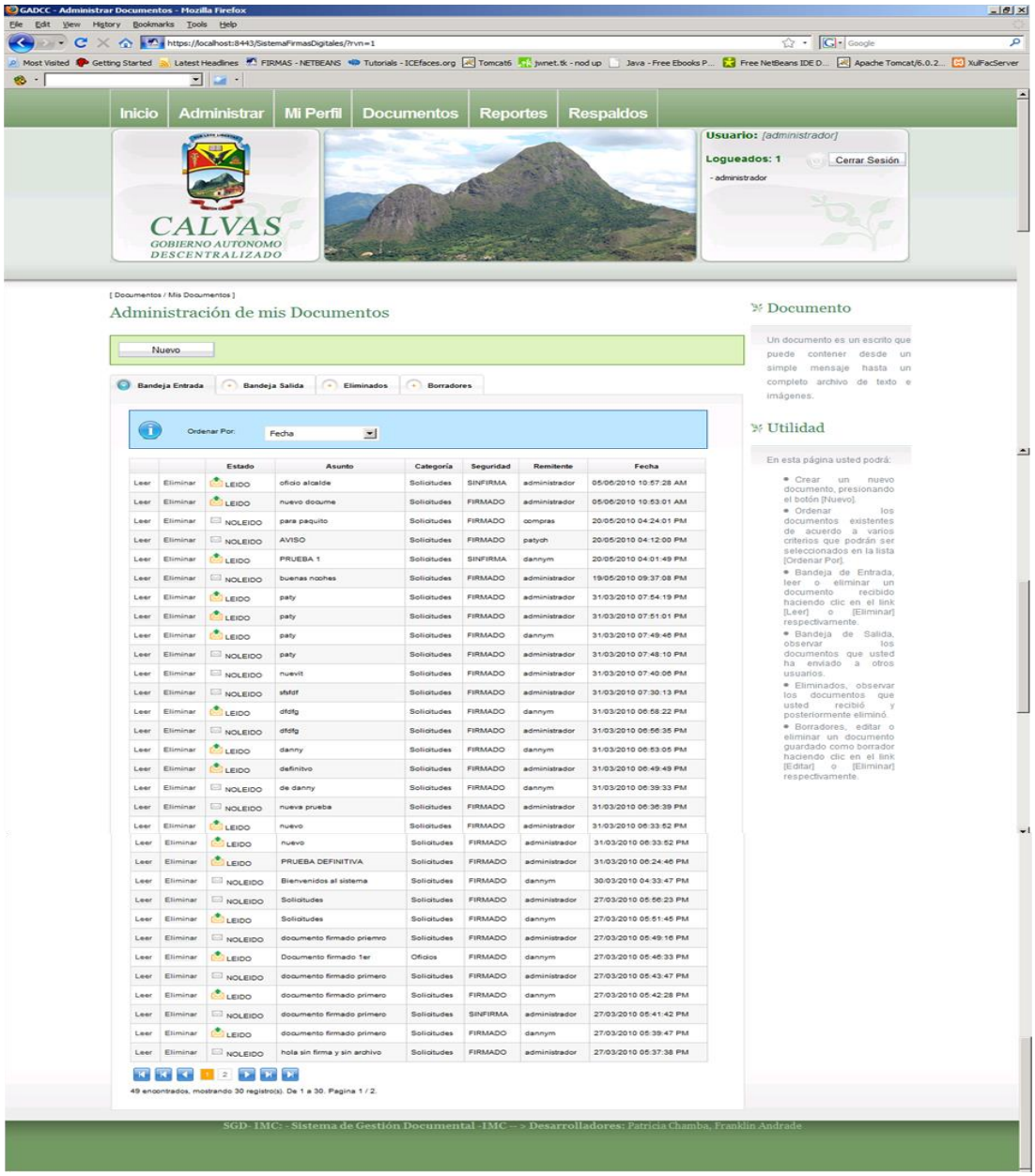


Fig. 45. Bandeja de Entrada

Mensaje de confirmación [Eliminar Documento bandeja de entrada]

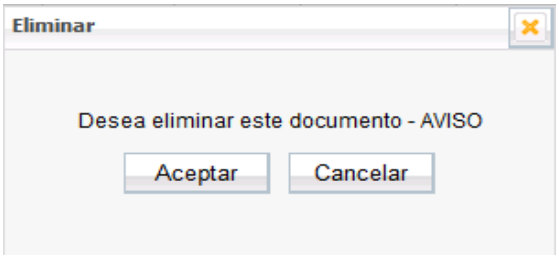


Fig. 46. Eliminar Bandeja de Entrada

Pag18: AdministrarDocumentos/sección Bandeja de salida

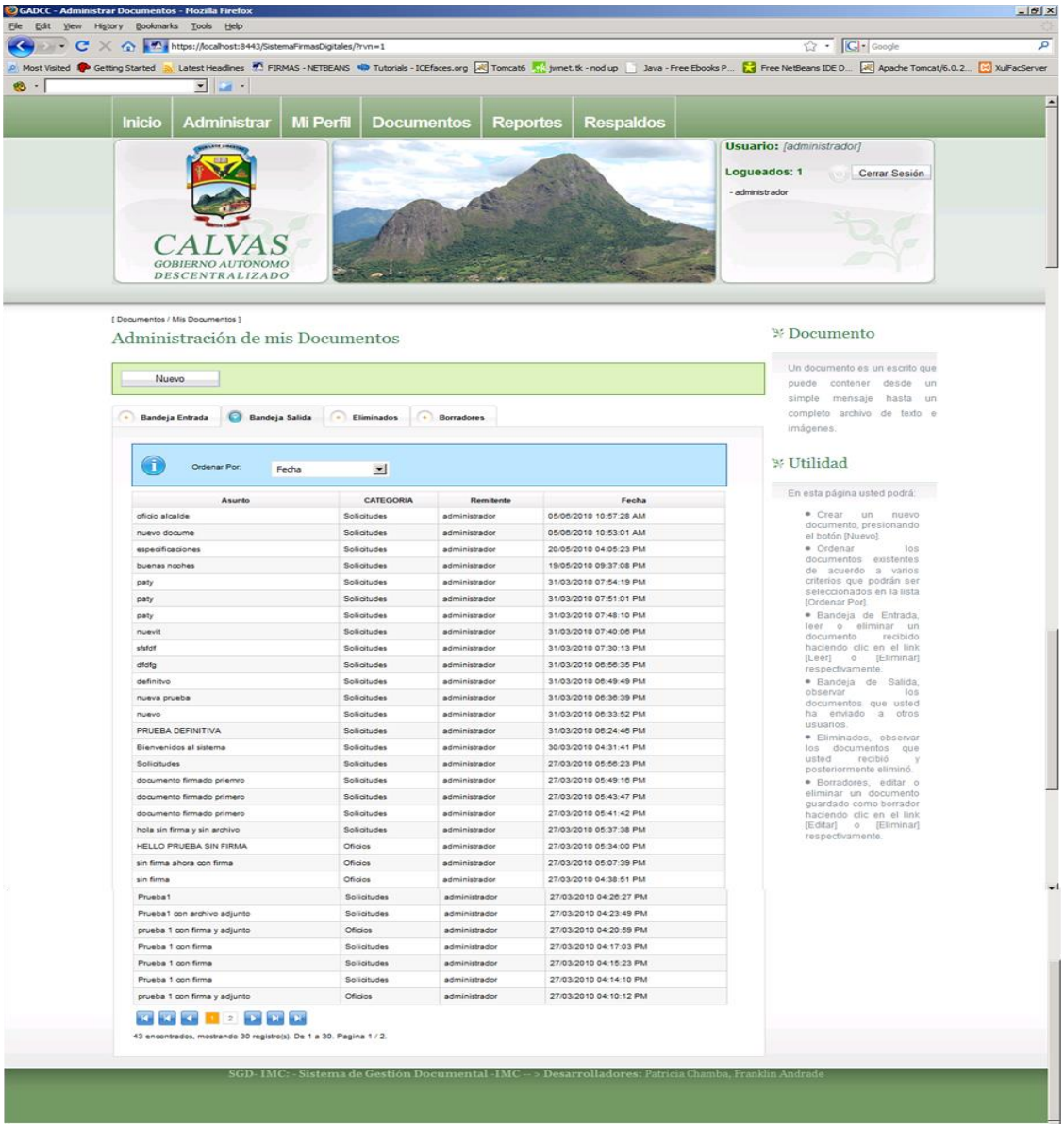


Fig. 47. Bandeja de Salida

Pag18: AdministrarDocumentos/sección Eliminados

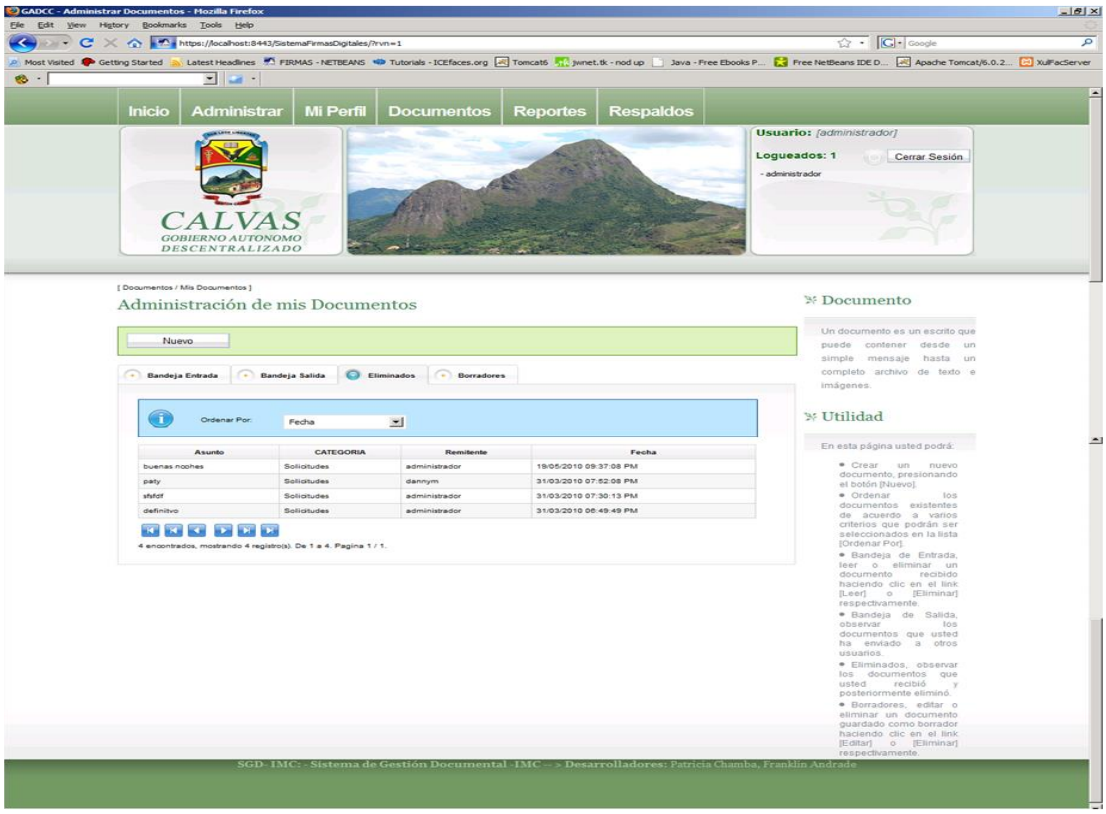


Fig. 48. Eliminados

Pag18: AdministrarDocumentos/sección Borradores

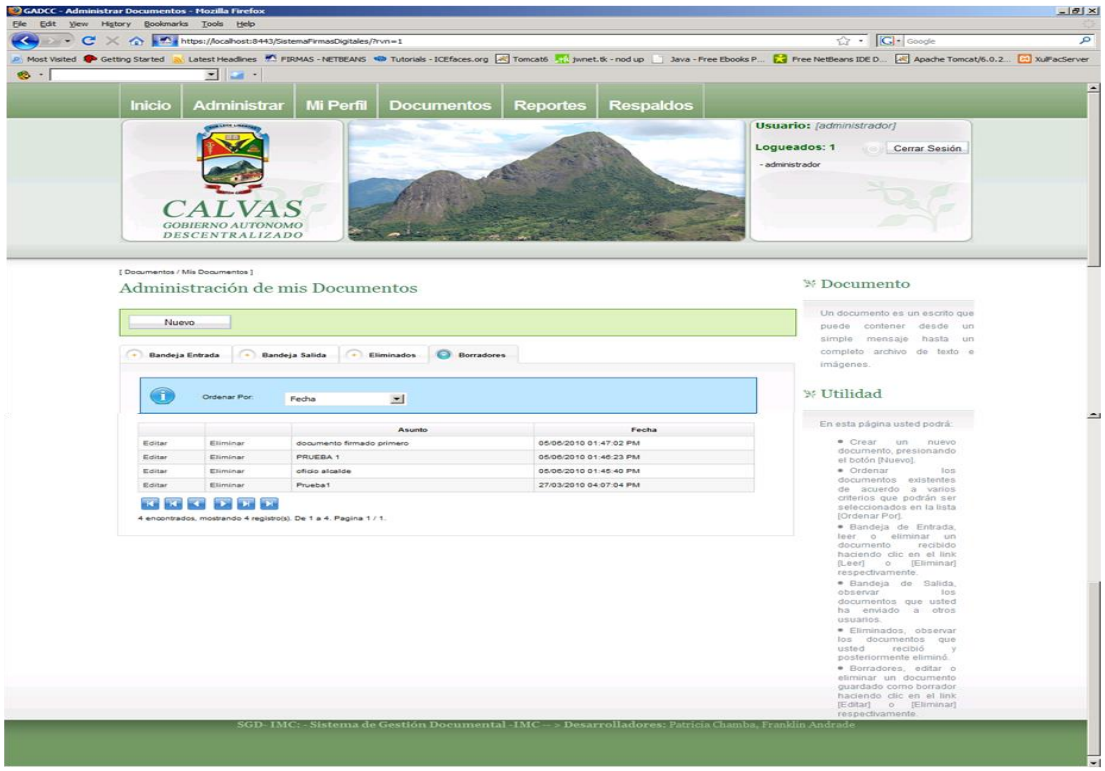


Fig. 49. Borradores

Mensaje de confirmación [Eliminar Borrador]

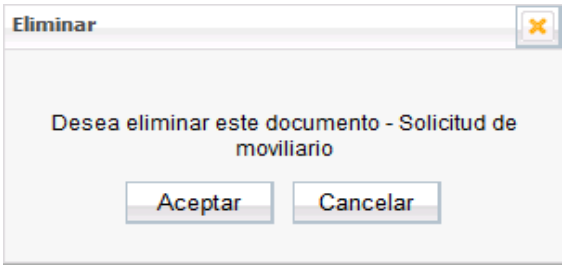


Fig. 50. Eliminar Borrador

Pag19: EditarDocumento

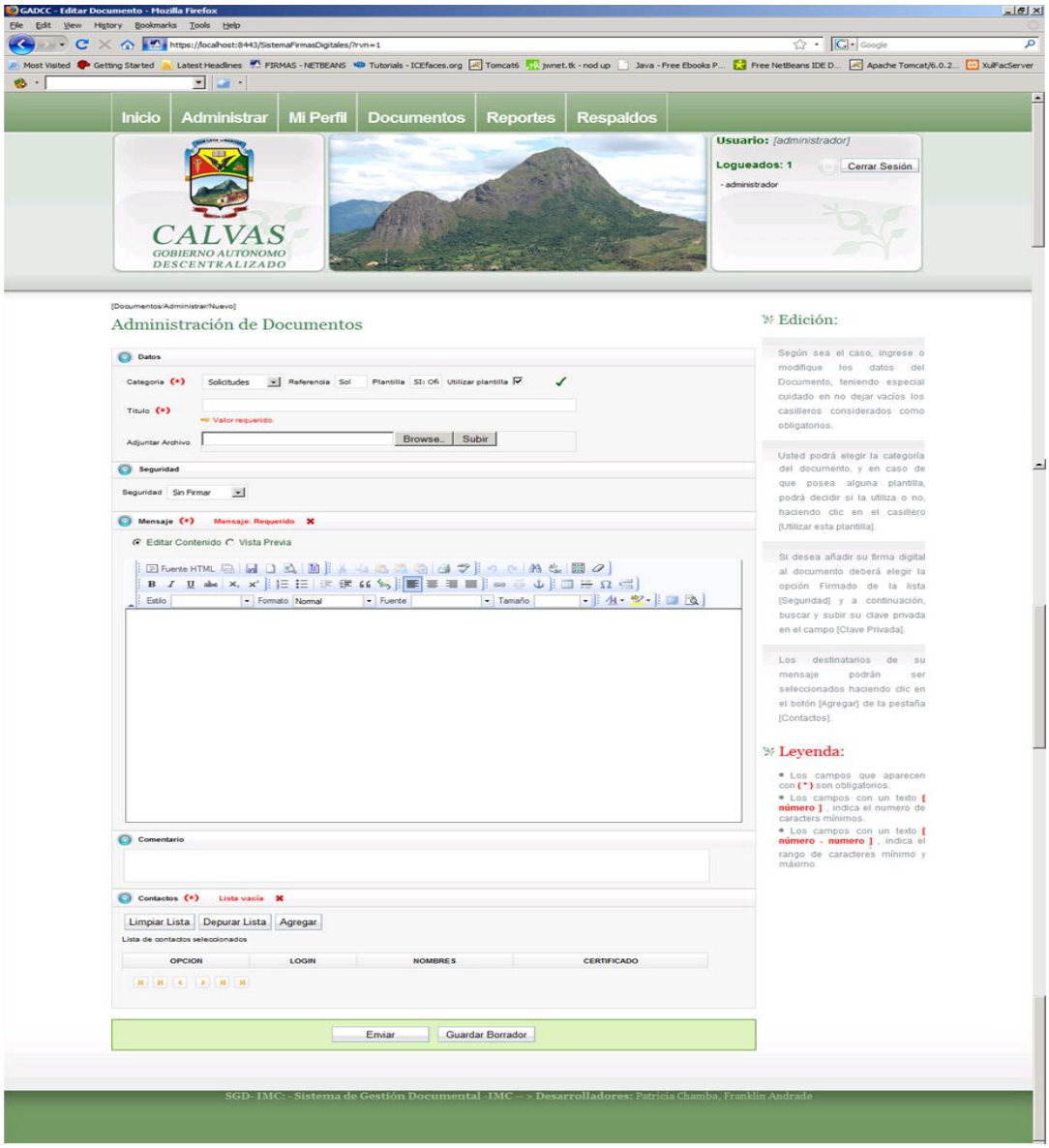


Fig. 51. Editar Documento

Diálogo [Directorio Archivo/Clave]

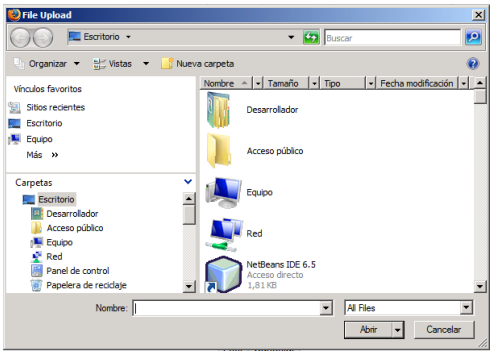


Fig. 52. Directorio de Archivo/Clave

Mensaje de error [No ha subido su clave privada]

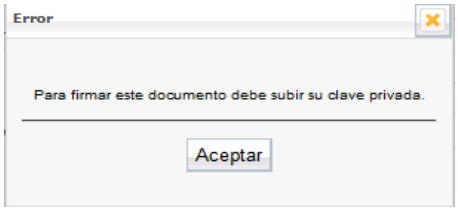


Fig. 53. Clave Privada no Subida

Mensaje de error [No ha especificado sus contactos]

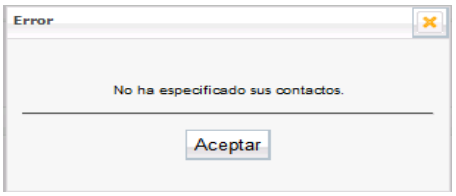


Fig. 54. Contactos no Especificados

Diálogo [Agregar Contacto]

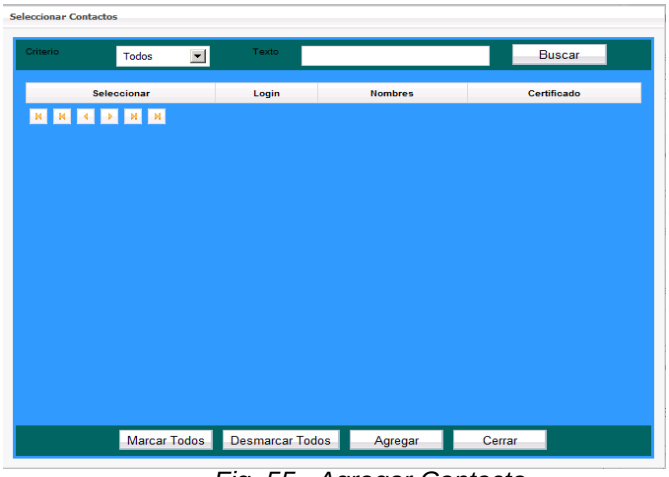


Fig. 55. Agregar Contacto

Mensaje de error [Depure lista de contactos]

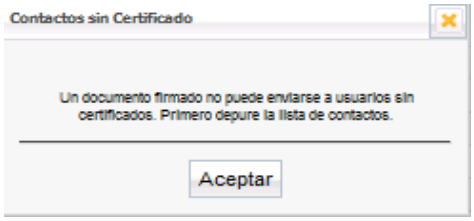


Fig. 56. Depurar Contactos

Pag20: Documentos

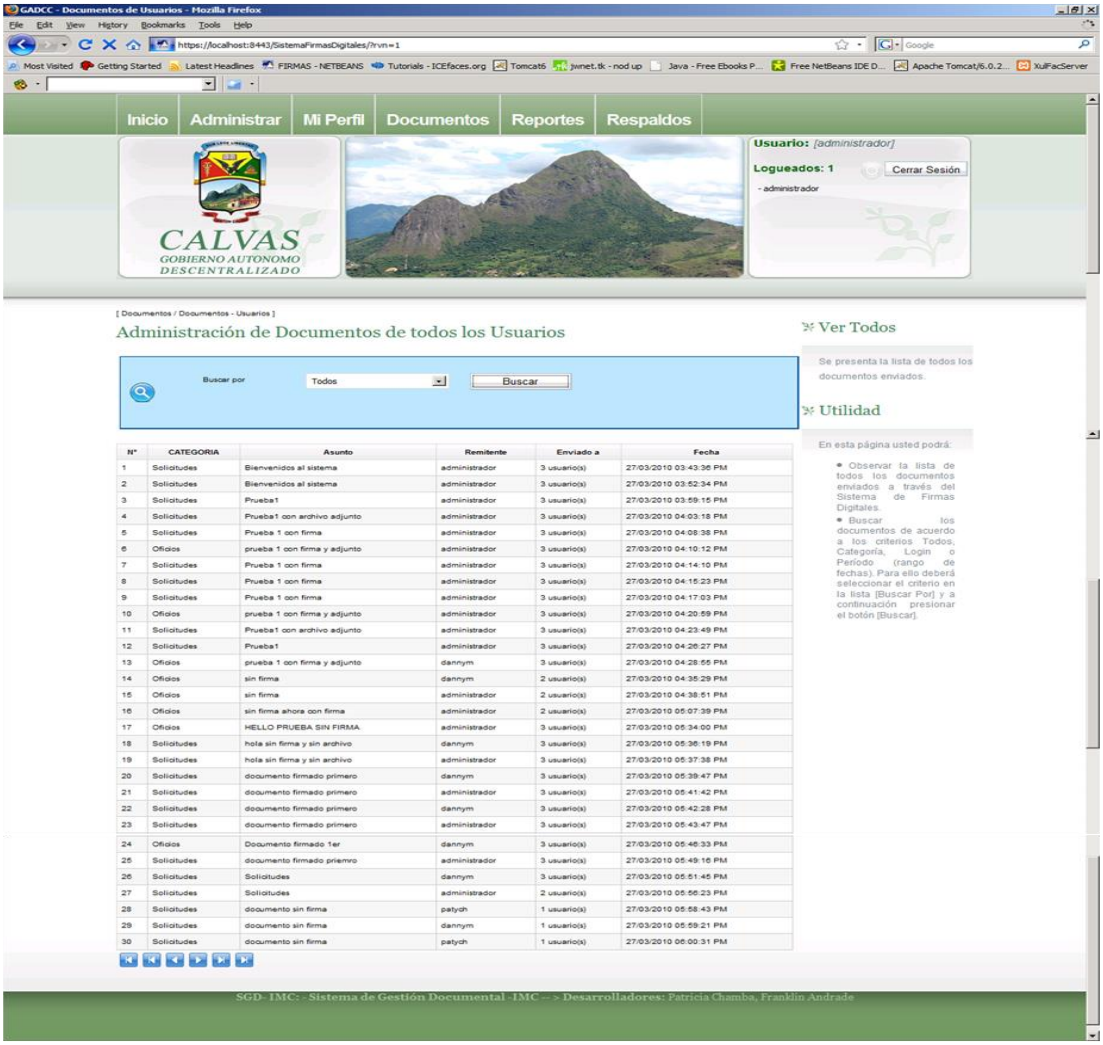


Fig. 57. Documentos

Pag21: DocumentoEnviado

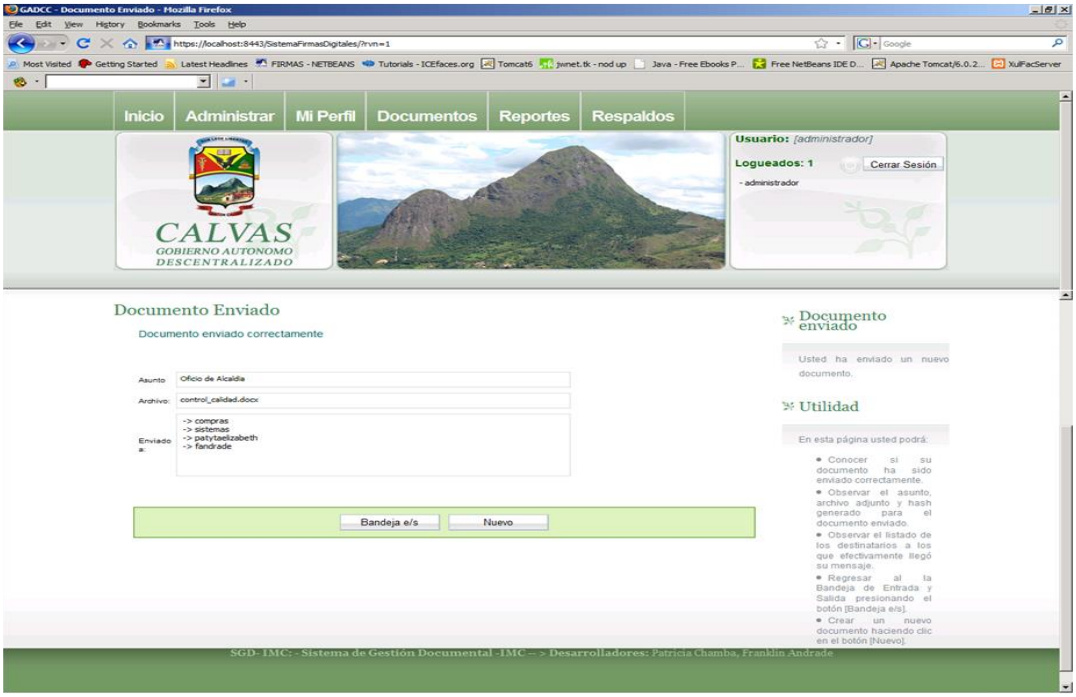


Fig. 58. Documento Enviado

Pag22: LeerDocumento

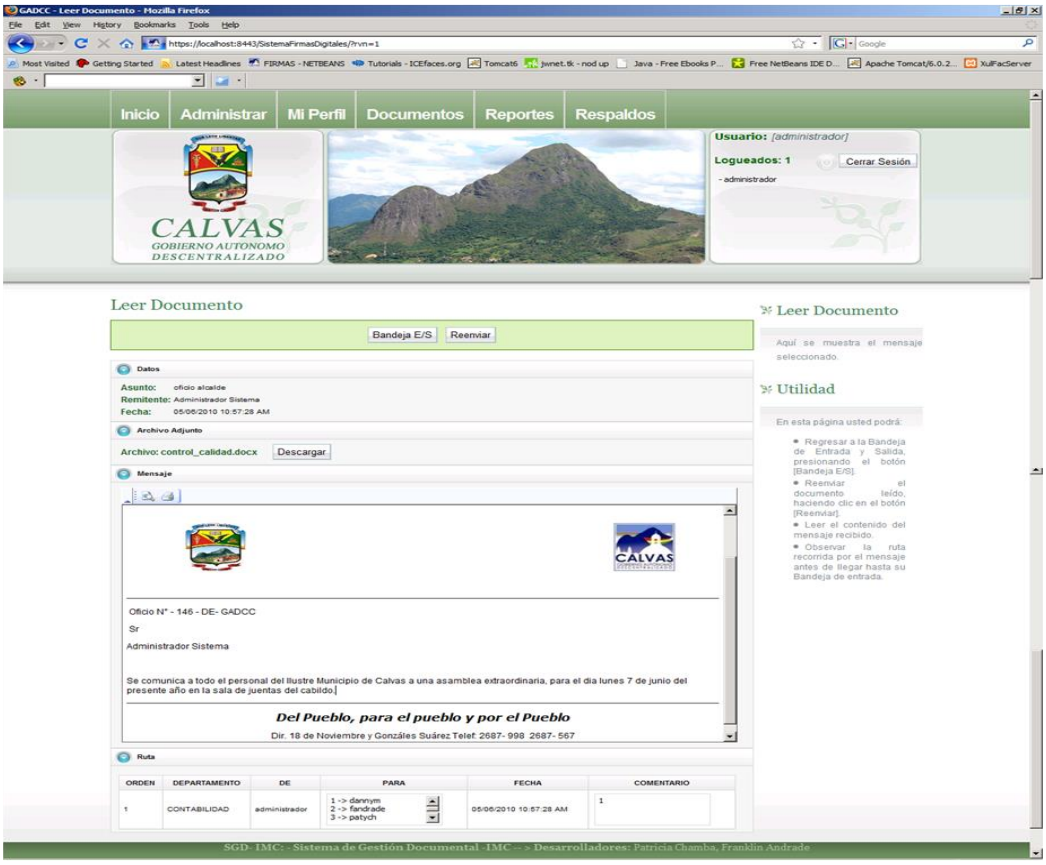


Fig. 59. Leer Documento

Diálogo [Descargar archivo adjunto]

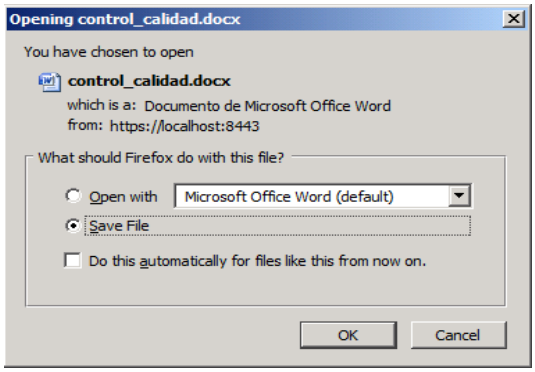


Fig. 60. Descargar Archivo Adjunto

Diálogo [Mensaje Firmado]

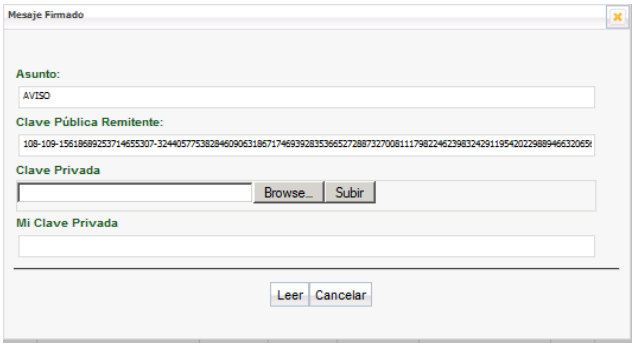


Fig. 61. Mensaje Firmado

Diálogo [Mensaje Auténtico]

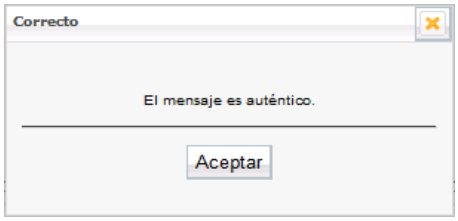


Fig. 62. Mensaje Auténtico

Diálogo [Mensaje Adulterado]

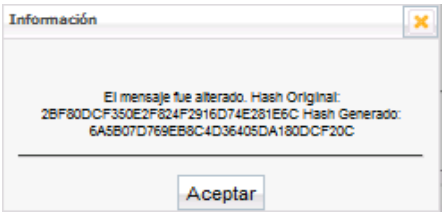


Fig. 63. Mensaje Adulterado

Pag23 [Reportes]

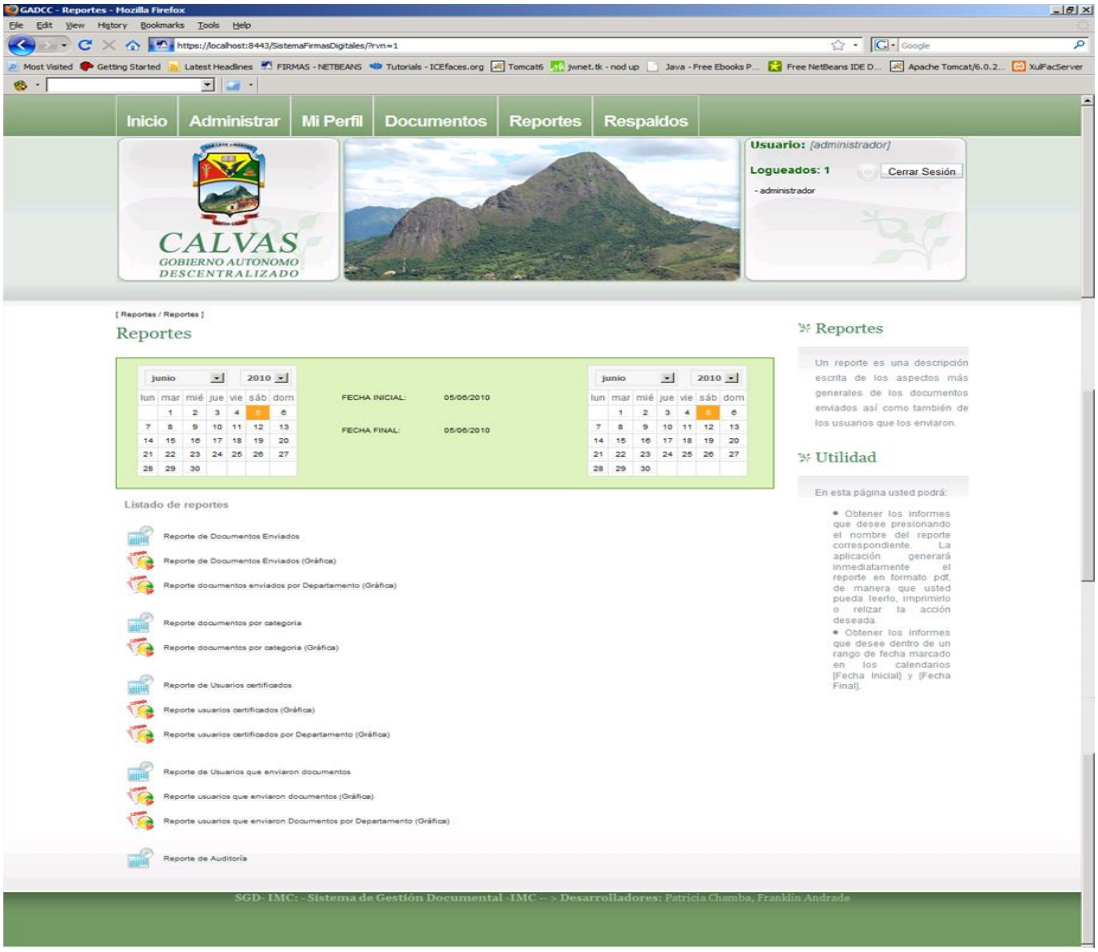


Fig. 64. Reportes

Reportes Escritos

N°	CATEGORÍA	SEGURIDAD	FECHA	SERIE	DESTINATARIOS	LEIDOS	NO LEIDOS	ARCHIVO ADJUNTO
1	Solicitudes	NO	03/06/2010		7	1	6	-
2	Solicitudes	NO	03/06/2010		7	1	6	patych.key
3	Solicitudes	SI	03/06/2010	CRT_GADCC-8	1	0	1	control_calidad.docx

Fig. 65. Reportes Escritos

Reportes Gráficos

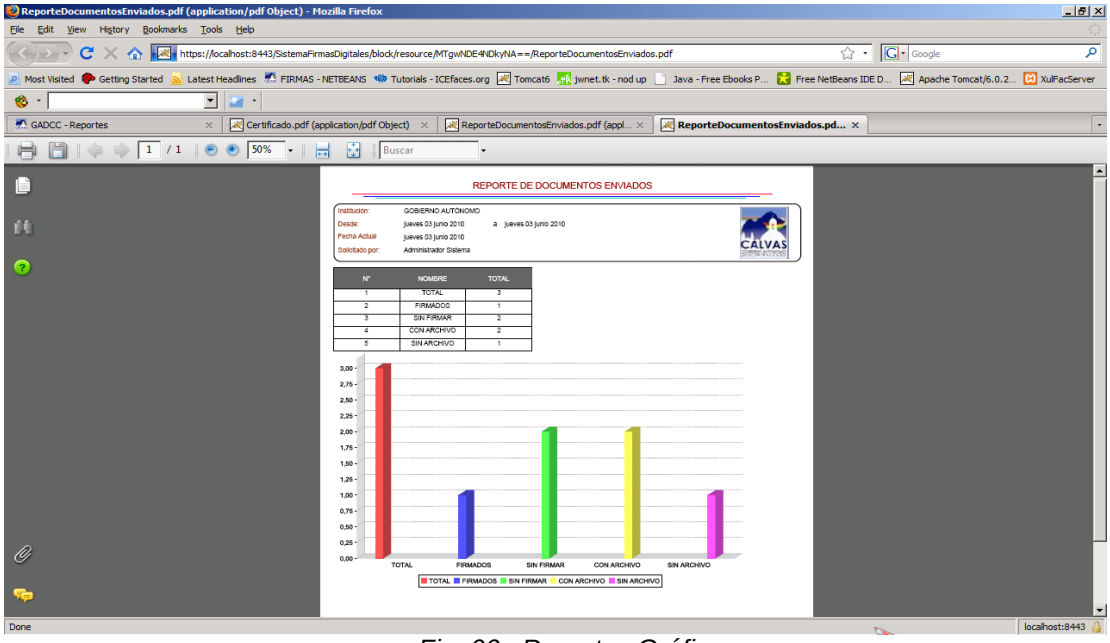


Fig. 66. Reportes Gráficos

Pag24 [Log]

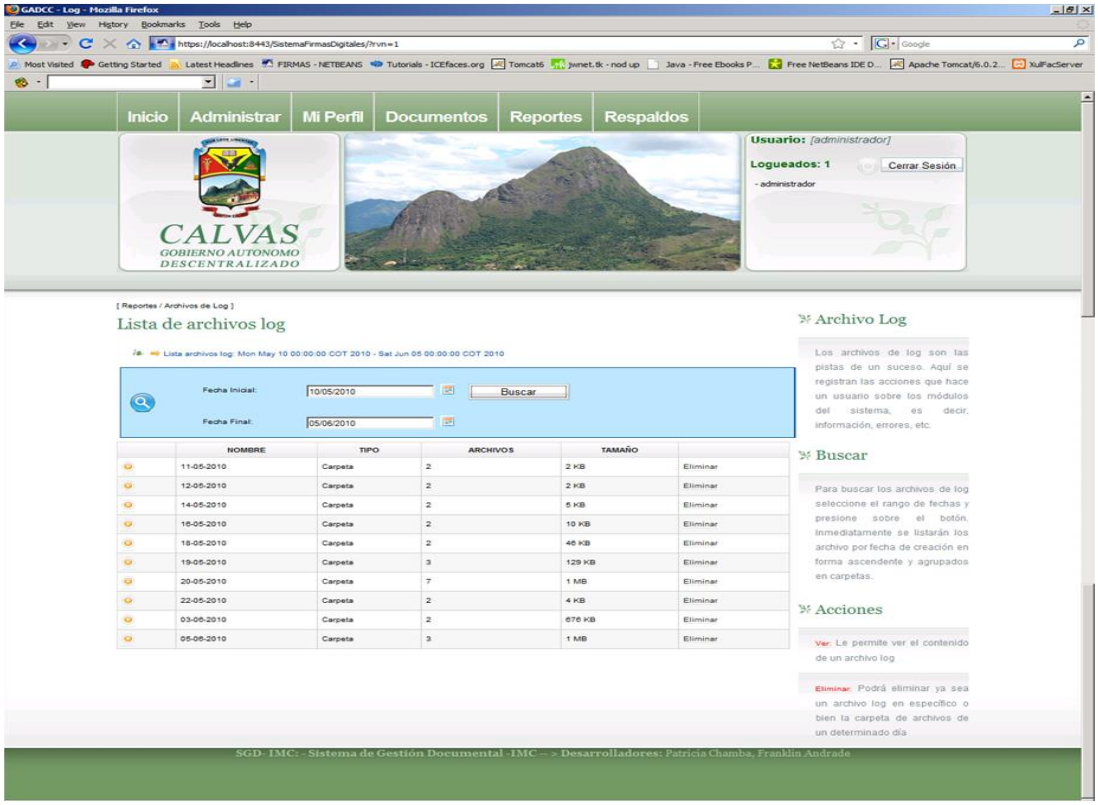


Fig. 67. Log

Mensaje de confirmación [Eliminar Log]

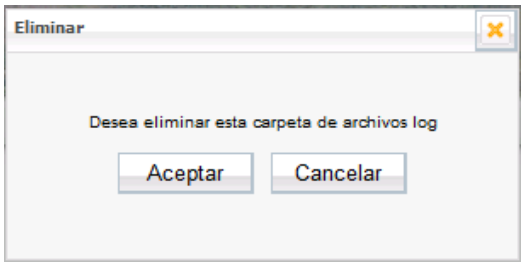


Fig. 68. Eliminar Log

Pag25 [VerLog]

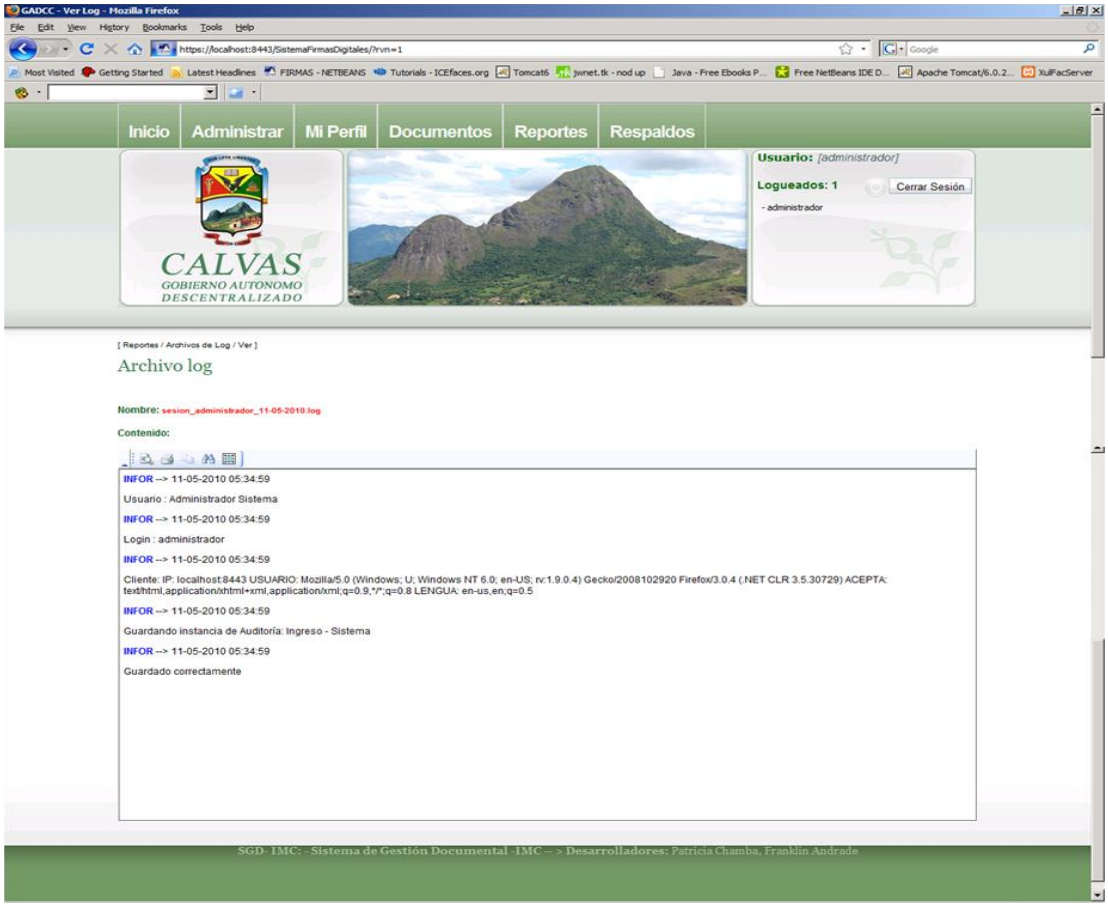


Fig. 69. Ver Log

Pag26 [Respaldos]

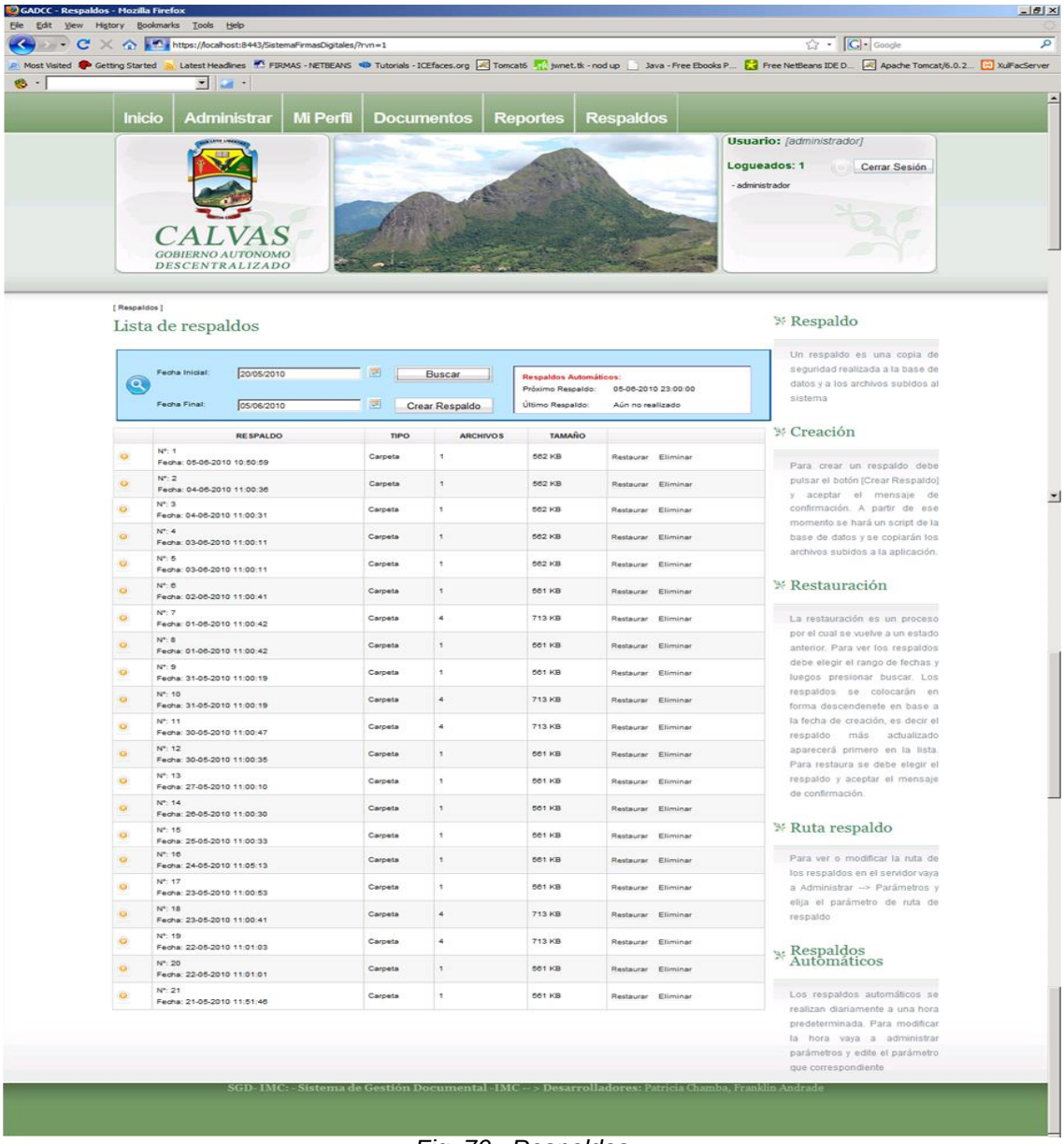


Fig. 70. Respaldos

Mensaje de confirmación [Eliminar Respaldo]

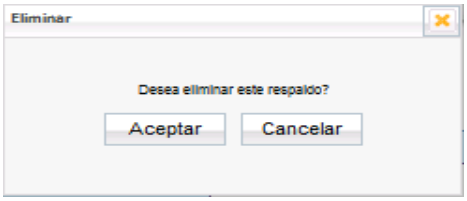


Fig. 71. Eliminar Respaldo

Dialogo [DiálogoEspere]

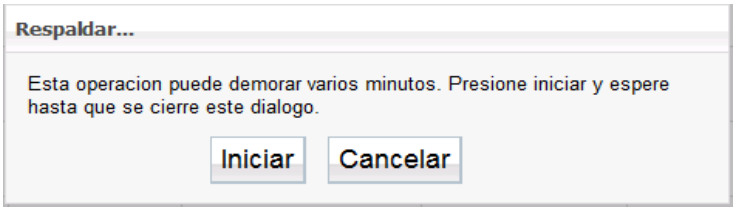


Fig. 72. Iniciar Respaldo

Diálogo [RestaurarRespaldo]

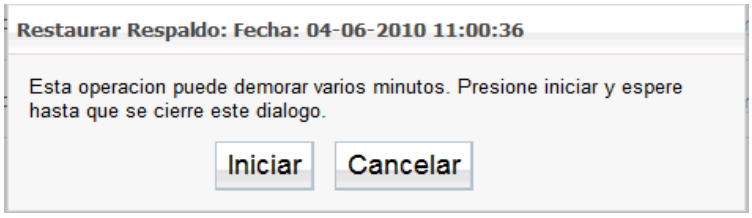


Fig. 73. Restaurar Respaldo

Diálogo [DiálogoFin]

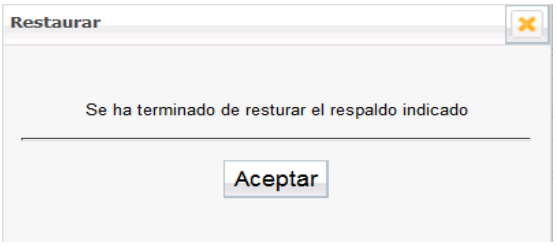


Fig. 74. Respaldo Terminado

8.8. DESCRIPCIÓN DE CASOS DE USO

Caso de Uso:	Logear Usuarios	**Código Caso de Uso:**	CU01
Meta:	Iniciar Sesión	**Código Meta:**	MT01
Propósito:	Iniciar sesión de un usuario		
Actor:	Administrador/Usuario		
Descripción:	El Administrador/Usuario ingresa su nombre de usuario y clave para iniciar una sesión en el sistema. En caso de que no recuerde su contraseña podrá guiarse por el indicio de la misma; además tendrá un número de 5 intentos como máximo para iniciar una sesión.		
Referencia a requerimientos:	RF01, RF02		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador/usuario haya ingresado al sistema. • El administrador/usuario haya activado la página [Pag01: Bienvenida] • Que el usuario/administrador que va a iniciar sesión se encuentre creado previamente en el sistema.		
Post condiciones:	• Gestionar Documentos Electrónicos • Cerrar Sesión.		

Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Elige opción[Iniciar Sesión] de la página[Pag01: Bienvenida]	2. Muestra la página[Pag02: IniciarSesión]
3. Ingresa su nombre de usuario en el fragmento [FLogin]	
4. Ingresa su clave.	
5. Elige opción [Iniciar Sesión]	6. Busca el usuario de acuerdo a su login ingresado en la base de datos [firmas]
	7. Valida que la clave ingresada sea la correcta.
	8. Verifica que el estado del usuario se encuentre activo en el sistema.
	9. Agrega el nuevo usuario logeado a la lista de usuarios logeados en el fragmento[FUsuariosConectados] de la página[Pag03: Inicio]
	10. Actualiza el fragmento [FUsuariosConectados] de todas las sesiones.

	11. Cumple con la meta: Auditar Logeo
	12. Muestra la página[Pag03: Inicio]
	13. La meta MT01 finaliza.
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Usuario no encontrado	
	A.6. Presenta un mensaje de validación indicando que el usuario no fue encontrado
	A.7. Incrementar el número de intentos para acceder al sistema en el fragmento [FLogin] de la página[Pag02:IniciarSesión]
	A.7. La meta continúa en el paso 3 del Curso Normal de Eventos.
B. Clave incorrecta	
	B.7. Presenta un mensaje de validación indicando que debe verificar su clave
	B.8. Muestra un texto indicando el indicio de la clave en el fragmento [FLogin]
	B.9. Incrementar el número de intentos para acceder al sistema en el fragmento [FLogin] de la página[Pag02: IniciarSesión]
	B.10. La meta continúa e n el paso 4 del Curso Normal de Eventos.
C. Número máximo de intentos sobrepasado	
	C.9. Presenta un mensaje de validación indicando que ha sobrepasado el máximo de intentos permitidos en el fragmento [FErrorLogin] de la página[Pag04:ErrorIniciar Sesión]
D. Usuario inactivo	
	D.8. El sistema presenta un mensaje de validación en el fragmento [FLogin] de la página [Pag02: IniciarSesión] indicando que el usuario está inactivo.
	D.9. La meta continúa en el paso 3 del Curso Normal de Eventos.

Tabla 10. Descripción de la meta: Iniciar Sesión

Caso de Uso:	Logear Usuarios	**Código Caso de Uso:**	CU01
Meta:	Cerrar Sesión	**Código Meta:**	MT02
Propósito:	Cerrar sesión de un usuario		
Actor:	Administrador/Usuario		
Descripción:	El Administrador/Usuario podrá cerrar su sesión en el momento que crea conveniente, una vez que haya ingresado al sistema. Por otro lado el sistema también cerrará la sesión del usuario si ésta ha caducado o expirado su tiempo de utilidad.		
Referencia a requerimientos:	RF01		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador/usuario haya ingresado al sistema y haya activado la página [Pag03: Inicio] • Que el usuario/administrador que va a iniciar sesión se encuentre creado previamente en el sistema.		
Post condiciones:	• Iniciar Sesión.		

Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Elige opción [Cerrar Sesión] del fragmento [FLog Off]	2. Cierra la sesión del usuario.
	3. Elimina el usuario de la lista de usuarios logeados del fragmento [FUsuariosConectados]
	4. Elimina archivos usados por los usuarios
	5. Actualiza el fragmento [FUsuariosConectados]
	6. Muestra la página[Pag01: Bienvenida]
	7. La meta MT02 finaliza.
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Sesión expirada	
	A.1. Presenta un mensaje de aviso indicando que la sesión ha caducado
A.2. Elige[Recargar]	A.3. Muestra la página[Pag01: Bienvenida]
	A.4. La meta MT02 finaliza

Tabla 11. Descripción de la meta: Cerrar Sesión

Caso de Uso:	Administrar Usuarios	**Código Caso de Uso:**	CU02
Meta:	Crear Usuario	**Código Meta:**	MT03
Propósito:	Crear nuevos usuarios		
Actor:	Administrador		
Descripción:	El Administrador podrá crear un nuevo usuario; para ello el sistema se encargará de verificar de que no exista el mismo, luego permitirá al administrador ingresar los datos correspondientes y almacenarlo en la base de datos[firmas]		
Referencia a requerimientos:	RF03		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página [Pag05: AdministrarUsuarios] • Cumplimiento de la meta: Iniciar Sesión		
Post condiciones:	• Crear Usuario • Editar Usuario • Eliminar Usuario		

Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Elige la opción [Nuevo] de la página [Pag05: AdministrarUsuarios].	2. Muestra la página[Pag06: EditarUsuarios]
3. Ingresa la cédula del usuario en el fragmento [FEditarUsuarios]	4. Valida cédula ingresada.
5. Ingresa los datos del nuevo usuario.	6. Valida que los campos requeridos no estén vacíos.
7. Ingresa el login del usuario	8. Valida que el login no haya sido ingresado.
9. Elige la opción[Guardar]	10. Guarda el nuevo usuario en la base de datos[firmas]
	11. Cumple con la meta: Auditar Creación de Usuario
	12. La meta MT03 finaliza
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Cédula incorrecta	
	A.4. Presenta mensaje de validación indicando que la cédula ingresada es incorrecta
	A.5. La meta continúa en el paso 3 del Curso Normal de Eventos.
B. Cédula duplicada	
	B.4. Presenta mensaje de validación indicando que la cédula ingresada ya ha sido registrada

	anteriormente.
	B.5. La meta continúa en el paso 3 del Curso Normal de Eventos.
C. Campos requeridos	
	C.6. El sistema presenta mensajes de validación indicando que los campos son requeridos.
	C.7. La meta continúa en el paso 4 del Curso Normal de Eventos.
D. Usuario duplicado	
	D.8. Presenta un mensaje de validación indicando que el login está duplicado.
	D.9. La meta continúa en el paso 7 del Curso Normal de Eventos.

Tabla 12. Descripción de la meta: Crear Usuario

Caso de Uso:	Administrar Usuarios	**Código Caso de Uso:**	CU02
Meta:	Buscar Usuario	**Código Meta:**	MT04
Propósito:	Buscar usuarios existentes		
Actor:	Administrador		
Descripción:	El Administrador selecciona el criterio de búsqueda, en base a ello ingresa el texto correspondiente a buscar; y con dicha información el sistema procederá a buscar a él o los usuarios.		
Referencia a requerimientos:	RF03		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema y haya activado la página [Pag05: AdministrarUsuarios] • Que exista por lo menos un usuario almacenado en la base de datos[firmas] • Cumplimiento de la meta: Iniciar Sesión.		
Post condiciones:	• Editar Usuario • Eliminar Usuario		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige el criterio de búsqueda del usuario en el fragmento[FAdministrarUsuarios] de la página[Pag05: Administrar Usuarios]			
2. Ingresa el texto de acuerdo al criterio de búsqueda elegido.			
3. Elige la opción[Buscar]		4. Busca el o los usuarios en la base de datos [firmas] de acuerdo al criterio elegido.	

	5. Muestra los datos del usuario/s encontrado/s en el fragmento [FAdministrarUsuarios]
	6. La meta MT04 finaliza.

Tabla 13. Descripción de la meta: Buscar Usuario

Caso de Uso:	Administrar Usuarios	**Código Caso de Uso:**	CU02
Meta:	Editar Usuario	**Código Meta:**	MT05
Propósito:	Editar usuarios existentes		
Actor:	Administrador		
Descripción:	El Administrador elige el usuario que desee modificar, para ello el sistema lo buscará previamente, una vez encontrado se podrá modificar los datos que se requieran del mismo.		
Referencia a requerimientos:	RF03		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página [Pag05: AdministrarUsuarios] • Que exista por lo menos un usuario almacenado en la base de datos[firmas] • Cumplimiento de la Meta: Buscar Usuario		
Post condiciones:	• Buscar Usuario. • Editar Usuario. • Eliminar Usuario.		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige la acción [Editar] en uno de los usuarios que se encuentran en el fragmento[FAdministrarUsuarios] de la página[Pag05: AdministrarUsuarios]		2. Carga y muestra los datos del usuario elegido en el fragmento [FEditarUsuario] de la página[Pag06: EditarUsuario]	
3. Edita la cédula del usuario en el fragmento [FEditarUsuarios]		4. Valida cédula modificada.	
5. Edita los datos del nuevo usuario en el fragmento		6. Valida que los campos requeridos no estén vacíos.	
7. Edita el login del usuario		8. Valida que el login no haya sido ingresado.	
9. Elige la opción[Guardar]		10. Guarda el nuevo usuario en la base de datos[firmas]	
		11. Cumple con la meta: Auditar Edición de Usuario.	
		12. La meta MT05 finaliza.	

Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Cambiar Estado del Usuario	
A.1. El administrador desactiva/activa el estado del usuario seleccionado en el fragmento[FAdministrarUsuarios] de la página [Pag05: AdministrarUsuarios]	A.2. Actualiza el estado del usuario en la base de datos[firmas]
	A.3. La meta MT05 finaliza.
B. Resetear clave	
B.3. Elige la opción [Resetear clave] en el fragmento [FEditarUsuario] de la página[Pag06: EditarUsuario]	B.4. Resetea la clave del usuario
	B.5. La meta MT05 finaliza.
C. Cédula incorrecta	
	C.4. Presenta mensaje de validación indicando que la cédula ingresada es incorrecta
	C.5. La meta continúa en el paso 3 del Curso Normal de Eventos.
D. Cédula duplicada	
	D.4. Presenta mensaje de validación indicando que la cédula ingresada ya ha sido ingresada anteriormente.
	D.5. La meta continúa en el paso 3 del Curso Normal de Eventos.
E. Campos requeridos	
	E.6. El sistema presenta mensajes de validación indicando que los campos son requeridos.
	E.7. La meta continúa en el paso 5 del Curso Normal de Eventos.
F. Usuario duplicado	
	F.8. Presenta un mensaje de aviso indicando que el login está duplicado.
	F.9. La meta continúa en el paso 7 del Curso Normal de Eventos.

Tabla 14. Descripción de la meta: Editar Usuario

Caso de Uso:	Administrar Usuarios	**Código Caso de Uso:**	CU02
Meta:	Cambiar Clave	**Código Meta:**	MT06
Propósito:	Cambiar clave de usuarios existentes		
Actor:	Administrador		
Descripción:	El Administrador elige el usuario del que desea modificar su clave, para ello el sistema lo buscará previamente, una vez encontrado se podrá modificar su clave.		
Referencia a requerimientos:	RF05		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • Cumplimiento de la Meta: Buscar Usuario • El administrador haya activado la página [Pag06: EditarUsuario] • Que exista por lo menos un usuario almacenado en la base de datos[firmas]		
Post condiciones:	• Buscar Usuario. • Resetear Clave • Editar Usuario. • Eliminar Usuario.		

Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Elige la opción[Cambiar clave] en el fragmento [FEditarUsuario] de la página[Pag06: EditarUsuario]	2. Muestra el fragmento [FcambiarClave]
3. Ingresa nueva clave	
4. Ingresa la clave anterior	
5. Confirma la clave	
6. Ingresa el indicio de la nueva clave	
7. Elige [Aceptar]	8. Verifica q la clave anterior sea la correcta.
	9. Verifica que la confirmación de la clave sea igual a la nueva clave.
	10. Encripta y actualiza la nueva clave con el algoritmo MD5
	11. Obtiene el hash de la nueva clave
	12. Transforma la cadena a hexadecimal.
	13. Muestra el fragmento [FEditarUsuario] de la página[Pag06: EditarUsuario]
	14. La meta MT06 finaliza.

A. Clave anterior incorrecta	
	A.5. El sistema presenta un mensaje de validación indicando que la clave anterior no es correcta.
	A.6. La meta continúa en el paso 4 del Curso Normal de Eventos
B. Confirmación de la nueva clave incorrecta	
	B.5. El sistema presenta un mensaje de validación indicando que la clave nueva no coincide con la confirmada.
	B.6. La meta continúa en el paso 4 del Curso Normal de Eventos

Tabla 15. Descripción de la meta: Cambiar Clave

Caso de Uso:	Administrar Usuarios	**Código Caso de Uso:**	CU02
Meta:	Eliminar Usuario	**Código Meta:**	MT07
Propósito:	Eliminar usuarios existentes		
Actor:	Administrador		
Descripción:	El Administrador elige el usuario que desee eliminar, para ello el sistema lo buscará previamente, una vez encontrado se podrá eliminar.		
Referencia a requerimientos:	RF03		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página [Pag05: AdministrarUsuarios] • Que exista por lo menos un usuario almacenado en la base de datos[firmas] • Cumplimiento de la Meta: Buscar Usuario		
Post condiciones:	• Buscar Usuario. • Crear Usuario. • Editar Usuario.		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige la acción [Eliminar] del fragmento[FAdministrarUsuarios] de la página[Pag05: AdministrarUsuarios]		2. Presenta mensaje de confirmación indicando si se desea eliminar el usuario seleccionado.	
3. Elige [Aceptar]		4. Elimina el usuario de la base	

	de datos [firmas].
	5. Verifica la información almacenada del usuario que se eliminará.
	6. Cumple con la meta: Auditar Eliminación de Usuario.
	7. La meta MT07 finaliza.
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Integridad Referencial	
	A.5. Si el sistema no elimina el usuario presenta un mensaje de aviso indicando que no se puede eliminar el usuario por integridad referencial.
	A.6. La meta MT07 finaliza.

Tabla 16. Descripción de la meta: Eliminar Usuario

Caso de Uso:	Administrar Usuarios	**Código Caso de Uso:**	CU02
Meta:	Editar Perfil	**Código Meta:**	MT08
Propósito:	Editar perfil del usuario		
Actor:	Administrador/Usuario		
Descripción:	El Administrador/usuario podrá editar su perfil en lo que se refiere a datos personales y dirección.		
Referencia a requerimientos:	RF03		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página [Pag03: Inicio] • Cumplimiento de la meta: Iniciar Sesión		
Post condiciones:	• Gestionar Documentos Electrónicos		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige [Mi Perfil] del menú principal de la página[Pag03: Inicio]		2. Busca los datos del usuario logeado.	
		3. Carga y muestra los datos del usuario elegido en el fragmento [FMiPerfil] de la página[Pag09: MiPerfil]	
4. Edita su cédula		5. Valida cédula ingresada.	
6. Edita información de su perfil.		7. Valida que la información requerida no esté vacía.	
8. Elige la opción [Guardar]		9. Actualiza la información del	

	usuario en la base de datos[firmas]
	10. La meta MT08 finaliza.
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Cédula incorrecta	
	A.4. Presenta mensaje de validación indicando que la cédula ingresada es incorrecta
	A.5. La meta continúa en el paso 3 del Curso Normal de Eventos.
B. Cédula duplicada	
	B.4. Presenta mensaje de validación indicando que la cédula ingresada ya ha sido ingresada anteriormente.
	B.5. La meta continúa en el paso 3 del Curso Normal de Eventos.
C. Campos requeridos	
	C.6. El sistema presenta mensajes de validación indicando que los campos son requeridos.
	C.7. La meta continúa en el paso 5 del Curso Normal de Eventos.

Tabla 17. Descripción de la meta: Editar Perfil

Caso de Uso:	Administrar Certificados	**Código Caso de Uso:**	CU03
Meta:	Crear Certificado	**Código Meta:**	MT09
Propósito:	Crear un nuevo certificado para el Usuario.		
Actor:	Administrador		
Descripción:	El Administrador podrá generar un nuevo certificado para el usuario que lo haya solicitado, siempre y cuando dicho usuario no disponga de ninguno activo. Al momento que un certificado es creado, automáticamente se generará tanto la clave pública como la privada, a través del algoritmo RSA.		
Referencia a requerimientos:	RF06, RF07, RF08, RF10		
Tipo de CU:	Primario		
Pre condiciones:	• El administrado haya ingresado al sistema. • Que el usuario que solicitó el certificado se encuentre creado previamente en el sistema. • Qué el usuario que solicitó el certificado se encuentre activo en el sistema.		

	• Qué el usuario que solicitó el certificado no disponga de ningún certificado activo. • El administrador haya activado la página [Pag05: AdministrarUsuarios] • Cumplimiento de la Meta: Buscar Usuario
Post condiciones:	• Crear Nuevo Certificado • Guardar Claves • Ver Certificado en .PDF • Dar de Baja Certificado

Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Elige [Ver] en uno de los usuarios del fragmento[FAdministrarUsuarios] de la página[Pag05: Administrar Usuarios]	2. Busca los certificados del usuario.
	3. Muestra y carga los datos de él o los certificados que el usuario dispone en el fragmento[FCertificados] de la página [Pag07: Certificados]
4. Elige la opción[Nuevo]	5. Verifica el estado del usuario en el sistema.
	6. Verifica si el usuario no dispone de un certificado activo
	7. Genera el nuevo certificado
	8. Construye dos primos fuertes P y Q
	9. Calcula su producto (N)
	10. Calcula Phi(n): =(p-1)(q-1)
	11. Calcula e, primo relativo Phi(n).
	12. Elige e>1 y lo va variando hasta que mcd(e,phi_n)=1 y mcd(e-1, phi_n)=2
	13. Calcula d: $(e)^{-1}$.mod(phi_n)
	14. Obtiene la clave pública (n,e) y la clave privada(n,d)
	15. Fija el nuevo certificado como válido
	16. Muestra la información del nuevo certificado en el fragmento [FEditarCertificado] de la página[Pag08: Editar Certificado]
17. Selecciona la fecha de expiración del nuevo	18. Valida la fecha de expiración

certificado	elegida
19. Elige[Guardar]	20. Guarda el nuevo certificado del usuario en la base de datos[firmas]
	21. Cumple con la meta: Auditar Creación de Certificado.
	22. Muestra los datos principales del nuevo certificado en el fragmento [FCertificados] de la página [Pag07: Certificados]
	23. La meta MT09 finaliza.
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Ver Certificado en PDF	
A.4. Elige [Ver] en uno de los certificados que se encuentran en el fragmento [FCertificados] de la página [Pag07: Certificados]	A.5. Muestra los datos del certificado en el fragmento[FEditarCertificado] de la página[Pag08: Editar Certificado]
A.6. Elige [PDF]	A.7. Muestra el certificado en formato .pdf
	A.8. La meta MT09 finaliza.
B. Guardar claves	
B.4. Elige [Ver] en uno de los certificados que se encuentran en el fragmento [FCertificados] de la página [Pag07: Certificados]	B.5. Muestra los datos del certificado en el fragmento[FEditarCertificado] de la página[Pag08: Editar Certificado]
B.6. Elige clave pública o privada	B.7. Genera un archivo con los datos de la clave elegida.
	B.8. Presenta un asistente para descargar el archivo generado.
B.9. Elige [OK] o [Guardar] según el navegador utilizado.	B.10. Muestra un diálogo con el directorio a elegir para almacenar las claves.
B.11. Selecciona directorio	
B.12. Elige[Aceptar]	B.13. Guarda las claves en el cliente.
	B.14. La meta MT09 finaliza.
C. Usuario Inactivo	
	C.5. Muestra un mensaje de aviso indicando que no se puede crear el certificado porque el usuario que lo solicita está inactivo en el sistema
C.6. Elige [Aceptar]	C.6. La meta MT09 finaliza.
D. Nuevo certificado disponiendo de uno activo	
	D.6. Muestra un mensaje de aviso indicando que el usuario ya

	dispone de un certificado activo.
D.7. Elige[Aceptar]	D.8. La meta MT09 finaliza.
E. Fecha de expiración igual a la creación	
	E.18. Muestra un mensaje de aviso indicando que la fecha de expiración debe ser mayor a la de creación.
	E.19. La meta MT09 continúa en el paso 17 del Curso Normal de Eventos.

Tabla 18. Descripción de la meta: Crear Certificado

Caso de Uso:	Administrar Certificados	**Código Caso de Uso:**	CU03
Meta:	Dar de Baja Certificado	**Código Meta:**	MT10
Propósito:	Dar de baja al certificado del usuario elegido.		
Actor:	Administrador		
Descripción:	El Administrador podrá dar de baja al certificado que disponga activo el usuario, para ello deberá ingresar el motivo de la baja y posteriormente el sistema actualizará el estado de dicho certificado conjuntamente con el estado de sus claves: pública y privada.		
Referencia a requerimientos:	RF06		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • Que el usuario que solicitó la baja del certificado se encuentre creado previamente en el sistema. • El administrador haya activado la página [Pag05 AdministrarUsuarios] • El usuario disponga por lo menos de un certificado activo. • Cumplimiento de la Meta: Buscar Usuario		
Post condiciones:	• Crear nuevo certificado. • Ver Certificado en .PDF		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige [Ver] en uno de los usuarios del fragmento[FAdministrarUsuarios] de la página[Pag05: AdministrarUsuarios]		2. Carga y muestra la página [Pag07: Certificados] con los certificados que el usuario dispone en el fragmento[FCertificados]	
3. Elige la opción [Dar Baja] en el certificado activo.		4. Muestra el diálogo[Confirmar Baja] en el que se debe	

	ingresar el motivo de la baja del certificado
5. Ingresa el motivo de la baja del certificado.	
6. Elige [Dar Baja] en el diálogo presentado.	7. Actualiza el estado del certificado en la base de datos[firmas]
	8. Cumple con la meta: Auditar Actualización de Certificado.
	9. Muestra y actualiza el estado del certificado en la página[Pag07: Certificados]
	10. La meta MT10 finaliza.

Tabla 19. Descripción de la meta: Dar de baja Certificado.

Caso de Uso:	Administrar Categorías	**Código Caso de Uso:**	CU04
Meta:	Crear Categoría	**Código Meta:**	MT11
Propósito:	Crear nuevas categorías		
Actor:	Administrador		
Descripción:	El Administrador crea una nueva categoría, para ello previamente el sistema verificará que no se duplique la misma, luego de lo cual podrá ingresar los datos correspondientes a la categoría que se creará.		
Referencia a requerimientos:	RF11		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página [Pag10: AdministrarCategorías]		
Post condiciones:	• Crear Categoría • Editar Categoría • Eliminar Categoría		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige la opción [Nueva] del fragmento [FAdministrarCategorias] en la página [Pag10: AdministrarCategorías]		2. Muestra la página [Pag11: EditarCategoria]	
3. Ingresa los datos de la nueva categoría			
4. Selecciona una plantilla del listado existente.			
5. Elige la opción[Guardar]		6. Valida que la información requerida no esté vacía.	
		7. Valida que el nombre de la categoría ingresado no exista.	

	8. Guarda la nueva categoría en la base de datos[firmas]
	9. Cumple con la meta: Auditar Creación de Categoría
	10. La meta MT11 finaliza
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Campos requeridos	
	A.6. El sistema presenta un mensaje de validación indicando que los campos son requeridos.
	A.7. La meta continúa en el paso 3 del Curso Normal de Eventos.
B. Nombre de categoría duplicada	
	B.7. Presenta un mensaje de validación indicando que el nombre de la categoría ha sido duplicado.
	B.8. La meta continúa en el paso 3 del Curso Normal de Eventos.

Tabla 20. Descripción de la meta: Crear Categoría

Caso de Uso:	Administrar Categorías	**Código Caso de Uso:**	CU04
Meta:	Editar Categoría	**Código Meta:**	MT12
Propósito:	Editar categorías existentes		
Actor:	Administrador		
Descripción:	El Administrador elige una categoría existente y modifica la información que se requiera de la misma.		
Referencia a requerimientos:	RF11		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página [Pag10: AdministrarCategorías] • Que exista por lo menos una categoría almacenada en la base de datos[firmas]		
Post condiciones:	• Guardar Categoría • Editar Categoría • Eliminar Categoría		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige la acción [Editar] en una de las categorías del fragmento[FAdministrarCategoría] de la		2. Muestra y carga los datos de la categoría seleccionada en el fragmento [FEditarCategoría] de	

página[Pag10: AdministrarCategorías]	la página[Pag11: EditarCategoría]
3. Modifica la información que desee.	
4. Elige la opción [Guardar]	5. Valida que la información ingresada no esté vacía.
	6. Valida que el nombre de la categoría ingresado no exista.
	7. Actualiza la información de la categoría modificada en la base de datos[firmas]
	8. Cumple con la meta: Auditar Edición de Categoría
	9. La meta MT12 finaliza.
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Campos requeridos	
	A.5. El sistema presenta mensajes de validación indicando que los campos son requeridos.
	A.6. La meta continúa en el paso 3 del Curso Normal de Eventos.
B. Nombre de categoría duplicada	
	B.6. Presenta un mensaje de aviso indicando que el nombre de la categoría ha sido duplicado.
	B.7. La meta continúa en el paso 3 del Curso Normal de Eventos.

Tabla 21. Descripción de la meta: Editar Categoría

Caso de Uso:	Administrar Categorías	**Código Caso de Uso:**	CU04
Meta:	Eliminar Categoría	**Código Meta:**	MT13
Propósito:	Eliminar categorías existentes		
Actor:	Administrador		
Descripción:	El Administrador elige una categoría existente y la elimina en caso de ser necesario.		
Referencia a requerimientos:	RF11		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página [Pag10: AdministrarCategorías] • Que exista por lo menos una categoría almacenada en la base de datos[firmas]		

Post condiciones:	• Crear Categoría • Editar Categoría • Eliminar Categoría
Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Elige la acción [Eliminar] de una de las categorías del fragmento[FAdministrarCategoría] de la página[Pag10: AdministrarCategorías]	2. Presenta mensaje de confirmación indicando si se desea eliminar la categoría seleccionada.
3. Elige [Aceptar] del mensaje de confirmación.	4. Elimina la categoría seleccionada de la base de datos[firmas]
	5. Verifica si la categoría contiene documentos.
	6. Cumple con la meta: Auditar Eliminación de Categoría
	7. La meta MT13 finaliza.
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Categoría contiene documentos	
	A.5. El sistema presenta un mensaje de aviso indicando que no se puede eliminar la categoría porque contiene documentos.
A.6. Elige[Aceptar]	A.7. La meta continúa en el paso 1 del Curso Normal de Eventos.

Tabla 22. Descripción de la meta: Eliminar Categoría

Caso de Uso:	Administrar Plantillas	**Código Caso de Uso:**	CU05
Meta:	Crear Plantilla	**Código Meta:**	MT14
Propósito:	Crear nuevas plantillas		
Actor:	Administrador		
Descripción:	El Administrador crea una nueva plantilla, para ello previamente el sistema verificará que no se duplique la misma, luego de lo cual podrá ingresar los datos e imágenes correspondientes a la plantilla que se creará.		
Referencia a requerimientos:	RF12		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página [Pag12: AdministrarPlantillas]		

Post condiciones:	• Crear Plantilla • Editar Plantilla • Eliminar Plantilla
Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Elige la opción [Nueva] del fragmento [FAdministrarPlantillas] en la página [Pag12: AdministrarPlantillas]	2. Muestra la página [Pag13: EditarPlantilla]
3. Ingresa el nombre de la plantilla.	
4. Crea el encabezado y pie de la plantilla con las opciones de ayuda que se encuentran en el fragmento [FEditarPlantilla]	
5. Elige la opción[Guardar]	6. Valida que el nombre de la plantilla no esté vacio.
	7. Valida que el nombre de la plantilla ingresada no exista.
	8. Guarda la nueva plantilla en la base de datos[firmas]
	9. Cumple con la meta: Auditar Creación de Plantilla.
	10. La meta MT14 finaliza
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Crear plantilla a partir de las opciones de [Ayuda]	
A.4. Elige un [Token] de la lista de tokens de la sección [Ayuda]. Que se encuentra en el fragmento [FEditarPlantilla]	
A.5. Elige [+Encabezado] o [+Pie]	A.6. El sistema carga el token seleccionado en el área [Encabezado]o en el área [Pie] según lo que haya elegido.
A.7. Elige la opción [Guardar]	A.8. La meta continúa en el paso 6 del Curso Normal de Eventos.
B. Campos requeridos	
	B.6. El sistema presenta un mensaje de validación indicando que el campo es requerido.
	B.7. La meta continúa en el paso 3 del Curso Normal de Eventos.
C. Nombre de plantilla duplicada	
	C.7. Presenta un mensaje de

	validación indicando que el nombre de la plantilla ha sido duplicado.
	C.8. La meta continúa en el paso 3 del Curso Normal de Eventos.

Tabla 23. Descripción de la meta: Crear Plantilla

Caso de Uso:	Administrar Plantillas	**Código Caso de Uso:**	CU05
Meta:	Editar Plantilla	**Código Meta:**	MT15
Propósito:	Editar plantillas existentes		
Actor:	Administrador		
Descripción:	El Administrador elige una plantilla existente y modifica la información que se requiera de la misma.		
Referencia a requerimientos:	RF12		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página [Pag12: AdministrarPlantillas] • Que exista por lo menos una categoría almacenada en la base de datos[firmas]		
Post condiciones:	• Guardar Plantilla • Editar Plantilla • Eliminar Plantilla		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige la acción [Editar] en una de las plantillas del fragmento[FAdministrarPlantillas] de la página[Pag12: AdministrarPlantillas]		2. Muestra y carga los datos de la plantilla seleccionada en el fragmento[FEditarPlantilla] de la página[Pag13: EditarPlantilla]	
3. Modifica la información que desee.			
4. Elige la opción [Guardar]		5. Valida que el nombre de la plantilla no esté vacío.	
		6. Valida que el nombre de la plantilla ingresado no exista.	
		7. Actualiza la información de la plantilla modificada en la base de datos[firmas]	
		8. Cumple con la meta: Auditar Edición de Plantilla.	

	9. La meta MT15 finaliza.
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Editar plantilla a partir de las opciones de [Ayuda]	
A.3. Elige un [Token] de la lista de tokens de la sección [Ayuda]. Que se encuentra en el fragmento [FEditarPlantilla]	
A.4. Elige [+Encabezado] o [+Pie]	A.5. El sistema carga el token seleccionado en el área [Encabezado] o en el área [Pie] según lo que haya elegido.
A.6. Elige la opción [Guardar]	A.7. La meta continúa en el paso 6 del Curso Normal de Eventos.
B. Campos requeridos	
	B.5. El sistema presenta un mensaje de validación indicando que el campo es requerido.
	B.6. La meta continúa en el paso 3 del Curso Normal de Eventos.
C. Nombre de plantilla duplicada	
	C.6. Presenta un mensaje de aviso indicando que el nombre de la plantilla ha sido duplicado.
	C.7. La meta continúa en el paso 3 del Curso Normal de Eventos.

Tabla 24. Descripción de la meta: Editar Plantilla

Caso de Uso:	Administrar Plantillas	**Código Caso de Uso:**	CU05
Meta:	Eliminar Plantilla	**Código Meta:**	MT16
Propósito:	Eliminar plantillas existentes		
Actor:	Administrador		
Descripción:	El Administrador elige una plantilla existente y la elimina en caso de ser necesario.		
Referencia a requerimientos:	RF12		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página [Pag12: AdministrarPlantillas] • Que exista por lo menos una plantilla almacenada en la base		

	de datos[firmas]
Post condiciones:	• Crear Plantilla • Editar Plantilla • Eliminar Plantilla
Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Elige la acción [Eliminar] de una de las plantillas del fragmento [FAdministrarPlantillas] de la página[Pag12: AdministrarPlantillas]	2. Presenta mensaje de confirmación indicando si se desea eliminar la plantilla seleccionada.
3. Elige [Aceptar] en el mensaje de confirmación.	4. Elimina la plantilla seleccionada de la base de datos[firmas]
	5. Verifica si la plantilla esta asignada a alguna categoría.
	6. Cumple con la meta: Auditar Eliminación de Plantilla
	7. La meta MT16 finaliza.
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Plantilla esta asignada a un departamento	
	A.5. El sistema presenta un mensaje de aviso indicando que no se puede eliminar la plantilla porque esa asignada a una categoría.
A.6. Elige[Aceptar]	A.7. La meta continúa en el paso 1 del Curso Normal de Eventos.

Tabla 25. Descripción de la meta: Eliminar Plantilla

Caso de Uso:	Administrar Departamentos	**Código Caso de Uso:**	CU06
Meta:	Crear Departamento	**Código Meta:**	MT17
Propósito:	Crear nuevos departamentos		
Actor:	Administrador		
Descripción:	El Administrador crea un nuevo departamento para ello previamente el sistema verificará que no se duplique el mismo, luego de lo cual podrá ingresar los datos correspondientes al departamento que se creará		
Referencia a requerimientos:	RF13		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página [Pag14: AdministrarDepartamentos]		
Post	• Crear Departamento		

condiciones:	• Editar Departamento • Eliminar Departamento
Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Elige la opción [Nuevo] del fragmento [FAdministrarDepartamentos] de la página[Pag14: Administrar Departamentos]	2. Muestra la página[Pag15: EditarDepartamento]
3. Ingresa los datos del nuevo departamento	
4. Elige la opción[Guardar]	5. Valida que la información ingresada no esté vacía.
	6. Valida que el nombre del departamento ingresado no exista.
	7. Guarda el nuevo departamento en la base de datos[firmas]
	8. Cumple con la meta: Auditar Creación de Departamento.
	9. La meta MT17 finaliza
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Campos requeridos	
	A.5. El sistema presenta mensajes de validación indicando que los campos son requeridos.
	A.6. La meta continúa en el paso 3 del Curso Normal de Eventos.
B. Nombre de departamento duplicado	
	B.6. Presenta un mensaje de aviso indicando que el nombre del departamento ha sido duplicado.
B.7. Elige[Aceptar]	B.8. La meta continúa en el paso 3 del Curso Normal de Eventos.

Tabla 26. Descripción de la meta: Crear Departamento

Caso de Uso:	Administrar Departamentos	**Código Caso de Uso:**	CU06
Meta:	Editar Departamento	**Código Meta:**	MT18
Propósito:	Editar departamentos existentes		
Actor:	Administrador		
Descripción:	El Administrador elige un departamento existente y modifica la información que se requiera del mismo.		
Referencia a requerimientos:	RF13		

Tipo de CU:	Primario
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página[Pag14: AdministrarDepartamentos] • Que exista por lo menos un departamento almacenado en la base de datos[firmas]
Post condiciones:	• Guardar Departamento • Editar Departamento • Eliminar Departamento
Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Elige la acción [Editar] de uno de las departamentos del fragmento [FAdministrarDepartamentos] de la página[Pag14: Administrar Departamentos]	2. Muestra y carga los datos del departamento seleccionado en el fragmento [FEditarDepartamento] de la página[Pag15: EditarDepartamento]
3. Modifica la información que desee.	
4. Elige la opción [Guardar]	5. Valida que la información ingresada no esté vacía.
	6. Valida que el nombre del departamento ingresado no exista.
	7. Actualiza la información del departamento modificado en la base de datos[firmas]
	8. Cumple con la meta: Auditar Edición de Departamento.
	9. La meta MT18 finaliza.
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Campos requeridos	
	A.5. El sistema presenta mensajes de validación indicando que los campos son requeridos.
	A.6. La meta continúa en el paso 3 del Curso Normal de Eventos.
B. Nombre de departamento duplicado	
	B.6. Presenta un mensaje de aviso indicando que el nombre del departamento ha sido duplicado.
B.7. Elige[Aceptar]	B.8. La meta continúa en el paso 3 del Curso Normal de Eventos.

Tabla 27. Descripción de la meta: Editar Departamento

Caso de Uso:	Administrar Departamentos	**Código Caso de Uso:**	CU06
Meta:	Eliminar Departamento	**Código Meta:**	MT19
Propósito:	Eliminar departamentos existentes		
Actor:	Administrador		
Descripción:	El Administrador elige un departamento existente y lo elimina en caso de ser necesario.		
Referencia a requerimientos:	RF13		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página[Pag14: AdministrarDepartamentos] • Que exista por lo menos un departamento almacenado en la base de datos[firmas]		
Post condiciones:	• Crear Departamento • Editar Departamento • Eliminar Departamento.		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige la acción [Eliminar] en uno de los departamentos del fragmento [FAdministrarDepartamentos] de la página[Pag14: Administrar Departamentos]		2. Presenta mensaje de confirmación indicando si se desea eliminar el departamento seleccionado.	
3. Elige [Aceptar] del mensaje de confirmación.		4. Elimina el departamento seleccionado de la base de datos[firmas]	
		5. Verifica si el departamento contiene usuarios.	
		6. Cumple con la meta: Auditar Eliminación de Departamento.	
		7. La meta MT19 finaliza.	
Curso Alterno de Eventos			
Acción del Actor		**Respuesta del Sistema**	
A. Departamento contiene usuarios			
		A.5. El sistema presenta un mensaje de aviso indicando que no se puede eliminar el departamento porque contiene usuarios.	
A.6. Elige[Aceptar]		A.7. La meta continúa en el paso 1 del Curso Normal de Eventos.	

Tabla 28. Descripción de la meta: Eliminar Departamento

Caso de Uso:	Administrar Parámetros	**Código Caso de Uso:**	CU07
Meta:	Editar Parámetros	**Código Meta:**	MT20
Propósito:	Editar parámetros de la aplicación		
Actor:	Administrador		
Descripción:	El Administrador elige un parámetro de la aplicación, como el nombre de la institución, siglas, perfil del certificado, entidad certificadora, ruta de la carpeta de respaldos, entre otros para luego proceder a editarlo según su conveniencia.		
Referencia a requerimientos:	RF14		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página[Pag17: EditarParámetro]		
Post condiciones:	• Guardar Parámetro • Editar Parámetro		

Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Elige la acción [Editar] de uno de las parámetros del fragmento [FEditarParametro] de la página[Pag16: AdministrarParámetros]	2. Muestra y carga los datos del parámetro seleccionado en la página [Pag17: EditarParámetro]
3. Modifica la información que desee del parámetro.	Valida que la información requerida no esté vacía.
4. Elige la opción [Guardar]	5. Actualiza la información del parámetro modificado en la base de datos[firmas]
	6. Cumple con la meta: Auditar Edición de Parámetro.
	7. La meta MT20 finaliza.
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Campos requeridos	
	A.5. El sistema presenta mensajes de validación indicando que los campos son requeridos.
	A.6. La meta continúa en el paso 3 del Curso Normal de Eventos.

Tabla 29. Descripción de la meta: Editar Parámetros

Caso de Uso:	Gestionar Documentos Electrónicos	**Código Caso de Uso:**	CU08
Meta:	Crear/Enviar Documentos	**Código Meta:**	MT21
Propósito:	Crear un nuevo documento		
Actor:	Administrador/Usuario		
Descripción:	El Administrador/usuario podrá crear un nuevo documento, el mismo que puede o no estar firmado, con o sin archivos adjuntos según sea la necesidad. En caso de que se desee enviar un documento firmado el sistema verificará que el remitente y sus destinatarios dispongan de un certificado activo.		
Referencia a requerimientos:	RF07, RF09, RF15, RF20, RF24		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador/usuario haya ingresado al sistema. • El administrador/usuario haya activado la página[Pag18: AdministrarDocumentos] • Que exista por lo menos una categoría almacenada en la base de datos [firmas]. • Qué el administrador/usuario en caso de querer enviar un documento firmado dispongan de un certificado activo y sin haber expirado. • Qué exista por lo menos un usuario almacenado en la base de datos[firmas]		
Post condiciones:	• Crear documento • Seleccionar contactos • Enviar documento • Leer documento • Eliminar documento de la bandeja entrada. • Crear un borrador. • Editar un borrador • Eliminar un borrador. • Presentar la bandeja de entrada. • Presentar la bandeja de salida. • Presentar los borradores. • Presentar documentos eliminados.		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige la opción [Nuevo] del fragmento[FAdministrarDocumentos] de la página[Pag18:AdministrarDocumentos]		2. Muestra la página [Pag19:EditarDocumento]	
3. Selecciona la categoría del documento en el fragmento[FNuevoDocumento]		4. Carga la referencia correspondiente a la categoría seleccionada.	

	5. Carga el nombre de la plantilla existente de acuerdo a la categoría elegida.
6. Ingresa el título del documento	7. Valida que se haya ingresado el título del documento.
8. Elige [Browser] o [Examinar] según el navegador.	9. Muestra un diálogo con el directorio a elegir para subir un archivo
10. Elige el archivo a subir	
11. Elige[Abrir] del cuadro de diálogo	12. Carga el archivo en el fragmento [FNuevoDocumento]
13. Elige[Subir]	14. Valida el tamaño del archivo a subir.
	15. Sube el archivo al servidor
	16. Muestra el nombre del archivo en el fragmento [FNuevoDocumento]
17. Selecciona la opción [Sin Firmar]	
18. Ingresa el mensaje del documento a enviar en el fragmento[FNuevoDocumento]	19. Valida que se haya ingresado el mensaje del documento
20. Ingresa el comentario del documento	
21. Elige [Agregar]	22. Hace referencia a la meta: Agregar Contacto.
23. Elige[Enviar]	24. Depura la lista de contactos
	25. Verifica si existen contactos agregados a la lista depurada.
	26. Genera el hash del mensaje.
	27. Encriptar el mensaje con un certificado por defecto.
	28. Asigna el número correspondiente al documento considerando a cada usuario al que será enviado.
	29. Guarda el documento considerando cada uno de los contactos seleccionados en la base de datos[firmas]
	30. Añade el documento actual a la bandeja de entrada de cada usuario.
	31. Cumple con meta: Auditar Creación de Documento.
	32. Muestra la página [Pag21: DocumentoEnviado] con información del documento enviado

	33. La meta MT21 finaliza.
Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Campos requeridos	
	A.7. El sistema presenta un mensaje de validación indicando que el campo es requerido.
	A.8. La meta continúa en el paso 6 del Curso Normal de Eventos.
	A.19. El sistema presenta un mensaje de validación indicando que el campo es requerido
	A.20. La meta continúa en el paso 18 del Curso Normal de Eventos.
B. Tamaño del archivo excede el rango permitido	
	B.14. Muestra un mensaje de validación indicando que el tamaño del archivo ha excedido el rango permitido.
	B.15. La meta continúa en el paso 8 del Curso Normal de Eventos.
C. Eliminar archivo adjunto	
C.17. Elige [Eliminar] en el fragmento [FNuevoDocumento]	C.18. Elimina el archivo del servidor
	C.19. Elimina el archivo del fragmento [FNuevoDocumento]
	C.20. La meta continúa en el paso 17 del Curso Normal de Eventos.
D. Firmar documento	
D.17. Selecciona [Firmado] en el fragmento[FNuevoDocumento] de la página[Pag19:EditarDocumento]	D.18. Verifica que el usuario disponga de un certificado. Caso contrario presentará un mensaje de aviso indicando que para enviar documentos firmados debe tener un certificado.
	D.19. Presenta un selector de fichero para ingresar la clave privada
D.20. Elige [Browser] o [Examinar] según el navegador.	D.21. Muestra un diálogo con el directorio a elegir para subir el archivo
D.22. Selecciona la clave privada	
D.23. Elige[Abrir] en el cuadro de diálogo	D.24. Carga la clave privada en el fichero del fragmento[FNuevoDocumento]
D.25. Elige[Subir] en el selector de fichero del	D.26. Valida que el formato de

fragmento[FNuevoDocumento]	archivo de clave sea correcto. Caso contrario presentará un mensaje de validación indicando que dicho formato es incorrecto.
	D.27. Valida que el usuario disponga de un certificado activo. Caso contrario presentará un mensaje de validación indicando que no puede firmar porque no dispone de un certificado activo.
	D.28. Valida que el archivo de clave corresponda al certificado activo del remitente. Caso contrario presentará un mensaje de validación indicando que el archivo especificado no le corresponde a su certificado activo.
	D.29. Valida que el certificado no esté vencido. Caso contrario presentará un mensaje de validación indicando que dicho certificado ha caducado.
	D.30. Sube el archivo de clave privada al servidor.
	D.31. Muestra un mensaje de validación indicando que la clave ha sido cargada correctamente.
D.32. Ingresa el mensaje del documento a enviar en el fragmento[FNuevoDocumento]	D.33. Valida que se haya ingresado el mensaje del documento. Caso contrario presentará un mensaje de validación indicando que dicho texto es un valor requerido.
D.34. Ingresa el comentario del documento	
D.35. Elige [Agregar]	D.36. Hace referencia a la meta: Agregar Contacto.
D.37. Elige[Enviar]	D.38. Depura la lista de contactos válidos.
	D.39. Verifica si existen contactos agregados a la lista depurada. En caso de que la lista quede vacía presentará un mensaje de error indicando que no ha especificado sus contactos.
	D.40. Depura la lista de contactos inválidos.
	D.41. Verifica si todos los contactos agregados a la lista disponen de

	certificado activo. Caso contrario presentará un mensaje de error indicando que un documento firmado no puede enviarse a usuarios sin certificado, que primero depure la lista.
	D.42. Verifica que se haya subido la clave privada del remitente. Caso contrario presentará un mensaje de error indicando que para firmar el documento debe subir su clave privada.
	D.43. Obtiene el hash del mensaje con el algoritmo MD5.
	D.44. Por cada contacto invoca a la meta: Encriptar con RSA.
	D.45. Guarda el documento considerando cada contacto en la base de datos[firmas]
	D.46. Asigna el número correspondiente al documento de cada usuario.
	D.47. Añade el documento actual a la bandeja de entrada de cada usuario.
	D.48. Cumple con la meta: Auditar Creación de Documento.
	D.49. Muestra la página [Pag21: DocumentoEnviado] con información del documento enviado
	D.50. La meta MT21 finaliza.
E. Vista Previa	
E.18. Elige [Vista Previa] en el fragmento[FNuevoDocumento]de la página [Pag19: EditarDocumento]	E.19. Verifica si la categoría del documento contiene una plantilla y si está activada la opción utilizar esta plantilla
	E.20. Compila el encabezado de la plantilla
	E.21. Compila el pie de página de la plantilla.
	E.22. Muestra el encabezado y pie de página de la plantilla en el mensaje del documento que se va a crear.
	E.23. La meta continúa en el paso 18 del Curso Normal de Eventos.

F. No existen contactos especificados	
	F.25. Presenta un mensaje de error indicando que no ha especificado sus contactos.
F.26. Elige[Aceptar]	F.27. La meta continúa en el paso 21 del Curso Normal de Eventos
G. Ver Bandeja Entrada/Salida	
G.33. Elige [Bandeja E/S] de la página[Pag21: DocumentoEnviado]	G.34. Muestra la página [Pag18:AdministrarDocumentos]
	G.35. La meta continúa en el paso 3 del Curso Normal de Eventos.
H. Crear documento una vez que se envió uno nuevo	
H.33. Elige la opción [Nuevo] de la página[Pag21: DocumentoEnviado]	H.34. Muestra la página[Pag19:EditarDocumento]
	H.35. La meta continúa en el paso 3 del Curso Normal de Eventos.

Tabla 30. Descripción de la meta: Crear/Enviar Documento

Caso de Uso:	Gestionar Documentos Electrónicos	**Código Caso de Uso:**	CU08
Meta:	Encriptar con RSA.	**Código Meta:**	MT22
Propósito:	Encriptar mensaje que se enviará con el algoritmo RSA.		
Actor:	Sistema		
Descripción:	El sistema se encargará de encriptar el mensaje original con la ayuda del algoritmo RSA. Todo este proceso se efectúa con la finalidad de que los mensajes enviados gocen de autenticidad y no sean adulterados.		
Referencia a requerimientos:	RF23		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento del Curso Alterno: Firmar Documentos		
Post condiciones:	Mensaje encriptado.		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene el certificado activo de cada contacto.	
		2. Obtiene y carga la clave pública del contacto.	
		3. Cifra el mensaje con la clave privada del firmante.	
		4. Cifra el mensaje con la clave pública del contacto.(destinatario)	

	5. La meta MT22 finaliza

Tabla 31. Descripción de la meta: Encriptar con RSA

Caso de Uso:	Gestionar Documentos Electrónicos	**Código Caso de Uso:**	CU08
Meta:	Buscar Contacto	**Código Meta:**	MT23
Propósito:	Buscar un contacto de la lista de usuarios almacenados.		
Actor:	Administrador/Usuario		
Descripción:	El Administrador/usuario podrá buscar el contacto que éste requiera.		
Referencia a requerimientos:	RF18		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador/usuario haya ingresado al sistema. • El administrador haya activado la página[Pag19:Editar Documento] • Qué exista por lo menos un usuario almacenado en la base de datos[firmas]		
Post condiciones:	• Agregar Contacto • Eliminar Contacto • Buscar Contacto		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige la opción[Agregar] en el fragmento[FNuevoDocumento] de la página[Pag19:EditarDocumento]		2. Muestra el fragmento[FSeleccionar Contactos]	
3. Elige el criterio de búsqueda			
4. Ingresa el texto a buscar de acuerdo al criterio de búsqueda elegido.			
5. Elige[Buscar]		6. Busca los usuarios de acuerdo al criterio elegido en la base de datos[firmas]	
		7. Busca la existencia de algún certificado activo del usuario en la base de datos[firmas]	
		8. Muestra los usuarios encontrados en el fragmento[FSeleccionar Contactos]	
		9. La meta MT23 finaliza	

Tabla 32. Descripción de la meta: Buscar Contacto

Caso de Uso:	Gestionar Documentos Electrónicos	**Código Caso de Uso:**	CU08
Meta:	Agregar Contacto	**Código Meta:**	MT24
Propósito:	Agregar uno o varios contactos como destinatarios de un mensaje.		
Actor:	Administrador/Usuario		
Descripción:	El Administrador/usuario podrá agregar uno o varios contactos como destinatarios de un mensaje, para ello previamente debe buscarlos.		
Referencia a requerimientos:	RF18		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador/usuario haya ingresado al sistema. • El administrador haya activado la página[Pag19: EditarDocumento] • Qué exista por lo menos un usuario almacenado en la base de datos[firmas] • Cumplimiento de la meta: Buscar Contacto		
Post condiciones:	• Buscar Contacto • Agregar Contacto • Eliminar Contacto		

Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Marca el o los contactos que se encuentran en el fragmento[FSeleccionarContactos] de la página[Pag19: EditarDocumento]	
2. Elige [Agregar]	3. Agrega el o los contactos a la lista de destinatarios del fragmento [FNuevoDocumento]
4. Elige [Cerrar] en el fragmento[FSeleccionarContactos]	5. Cierra y muestra la página[Pag19: EditarDocumento]
	6. La meta MT24 finaliza

Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Marcar Todos	
A.1. Elige [Marcar Todos] en el fragmento[FSeleccionarContactos]	A.2. Marca todos los contactos de la lista.
	A.3. La meta continúa en el paso 2 del Curso Normal de Eventos.
B. Desmarcar Todos	
B.1. Elige [Desmarcar Todos] en el fragmento[FSeleccionarContactos]	B.2. Desmarca todos los contactos de la lista
	B.3. La meta continúa en el paso 1 del Curso Normal de Eventos.

C. Cerrar	
C.1. Elige [Cerrar] en el fragmento[FSeleccionarContactos]	C.2. Cierra y muestra la página[Pag19: EditarDocumento]
	C.3. La meta MT24 finaliza

Tabla 33. Descripción de la meta: Agregar Contacto

Caso de Uso:	Gestionar Documentos Electrónicos	**Código Caso de Uso:**	CU08
Meta:	Eliminar Contacto	**Código Meta:**	MT25
Propósito:	Eliminar uno o varios contactos seleccionados como destinatarios de un mensaje.		
Actor:	Administrador/Usuario		
Descripción:	El Administrador/usuario podrá eliminar uno o varios contactos como destinatarios de un mensaje, para ello previamente debe agregar por lo menos uno de ellos.		
Referencia a requerimientos:	RF18		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador/usuario haya ingresado al sistema. • El administrador haya activado la página[Pag19: EditarDocumento] • Qué exista por lo menos un usuario almacenado en la base de datos[firmas] • Cumplimiento de la meta: Buscar Contacto		
Post condiciones:	• Buscar Contacto • Agregar Contacto • Eliminar Contacto		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige [Eliminar] en el fragmento[FNuevoDocumento] de la página[Pag19: EditarDocumento]		2. Elimina el contacto elegido	
		3. La meta MT25 finaliza	
Curso Alterno de Eventos			
Acción del Actor		**Respuesta del Sistema**	
A. Limpiar Lista			
A.1. Elige [Limpiar Lista] en el fragmento[FNuevoDocumento] de la página[Pag19: EditarDocumento]		A.2. Elimina todos los contactos de la lista.	
		A.3. La meta MT25 finaliza.	
B. Depurar Lista			
B.1. Elige [Depurar Lista] en el fragmento[FNuevoDocumento] de la		B.2. Verifica si el documento está firmado.	

página[Pag19: EditarDocumento]	
	B.3. Verifica si todos los contactos elegidos tienen un certificado activo.
	B.4. Elimina los contactos que no disponen de un certificado activo en el fragmento[FNuevoDocumento]
	B.5. La meta MT25 finaliza.

Tabla 34. Descripción de la meta: Eliminar Contacto

Caso de Uso:	Gestionar documentos electrónicos	**Código Caso de Uso:**	CU08
Meta:	Leer Documentos Recibidos	**Código Meta:**	MT26
Propósito:	Leer documentos recibidos.		
Actor:	Administrador/Usuario		
Descripción:	El Administrador/usuario podrá leer los documentos recibidos. En caso de que estén firmados el destinatario deberá ingresar su clave privada para que el sistema compruebe la autenticidad del mensaje y pueda leerlo, de lo contrario el mensaje permanecerá sin ser leído.		
Referencia a requerimientos:	RF17, RF21, RF22, RF23, RF24, RF25, RF26		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador/usuario haya ingresado al sistema. • El administrador haya activado la página[Pag18: AdministrarDocumentos] • Qué exista por lo menos un documento en la bandeja de entrada.		
Post condiciones:	• Eliminar Bandeja de Entrada. • Leer Documentos Recibidos		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige [Leer] en el fragmento[FAdministrarDocumentos] de la página[Pag18: AdministrarDocumentos]		2. Decodifica el documento con ayuda del certificado por defecto.	
		3. Descifra el mensaje con la clave privada del certificado por defecto	
		4. Actualiza a Leído el estado del documento.	
		5. Muestra el documento en el fragmento[FLeer] de la página [Pag22:LeerDocumento]	
		6. La meta MT26 finaliza	

Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Leer Documento Firmado	
A.1. Elige [Leer] en el fragmento[FAdministrarDocumentos] de la página[Pag18: AdministrarDocumentos]	A.2. Presenta el diálogo[Mensaje Firmado] en el que indica que se debe ingresar la clave privada para poder abrir el documento
A.3.Elige[Examinar] o [Browser] según el navegador	A.4.Muestra un diálogo con el directorio a elegir para buscar la clave privada.
A.5. Selecciona su clave privada	
A.6. Elige [Abrir]	
A.7. Elige [Subir] en el diálogo[Mensaje Firmado]	A.8. Valida que se haya seleccionado un archivo de clave. Caso contrario presentará un mensaje de validación indicando que no ha especificado el archivo de clave
	A.9. Valida que se haya seleccionado un archivo de clave privada. Caso contrario presentará un mensaje de validación indicando que el formato de archivo de clave privada es incorrecto.
	A.10. Obtiene el certificado activo del usuario
	A.11.Verifica si la clave privada elegida corresponde a la que se encuentra en el certificado activo del usuario.
	A.12. Verifica que el certificado del usuario no haya expirado.
	A.13. Sube el archivo de clave privada al servidor.
	A.14. Muestra en un mensaje de validación la clave privada del usuario que ha sido cargada.
A.15. Elige [Leer] en el diálogo[Mensaje Firmado]	A.16. Descifra el mensaje con la clave privada del receptor del documento.
	A.17. Descifra el mensaje con la clave pública del remitente.
	A.18. Genera el hash del mensaje desencriptado.

	A.19. Comprueba el hash obtenido con el hash recibido.
	A.20. Presenta un mensaje de aviso indicando que el mensaje es autentico. Caso contrario presentará un mensaje indicando que el documento fue adulterado.
	A.21. Actualiza a Leído el estado del documento en el fragmento [FAdministrarDocumentos]
	A.22. Muestra el documento en la página[Pag22:LeerDocumento]
	A.23. La meta MT26 finaliza.
B. Descargar archivo adjunto	
B.6. Elige[Descargar] en el fragmento[FLeer] de la página[Pag22:LeerDocumento]	B.7. Presenta un asistente para descargar el archivo recibido
B.8. Elige [OK] o [Guardar] según el navegador utilizado.	B.9. Muestra un diálogo con el directorio a elegir para almacenar el archivo.
B.10. Selecciona directorio	
B.11. Elige[Aceptar]	B.12. Guarda el archivo recibido en el cliente.
	B.13. La meta MT26 finaliza.
C. Ver Bandeja Entrada/Salida	
C.6. Elige [Bandeja E/S] en el fragmento[FLeer] de la página[Pag22:LeerDocumento]	C.7. Muestra la página[Pag18:AdministrarDocumentos]
	C.8. La meta MT26 finaliza.
D. Reenviar	
D.6. Elige [Reenviar] en el fragmento[FLeer] de la página[Pag22:LeerDocumento]	D.7. Carga el documento en el fragmento[FNuevoDocumento] de la página [Pag19:EditarDocumento]
	D.8. La acción continúa en el paso 1 de la meta: Agregar Contacto

Tabla 35. Descripción de la meta: Leer Documentos Recibidos

Caso de Uso:	Gestionar Documentos Electrónicos	**Código Caso de Uso:**	CU08
Meta:	Eliminar Bandeja de Entrada.	**Código Meta:**	MT27
Propósito:	Eliminar documentos de la bandeja de entrada.		
Actor:	Administrador/Usuario		
Descripción:	El Administrador/usuario podrá eliminar los documentos de la bandeja de entrada que él seleccione.		
Referencia a requerimientos:	RF27		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador/usuario haya ingresado al sistema. • El administrador/usuario haya activado la página[Pag18: AdministrarDocumentos] • Qué exista por lo menos un documento recibido en la bandeja de entrada.		
Post condiciones:	• Leer Documentos Recibidos. • Crear/ Enviar Documentos • Eliminar Bandeja de Entrada.		

Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Elige [Eliminar] en el fragmento[FAdministrarDocumentos] de la página[Pag18: AdministrarDocumentos]	2. Presenta un mensaje de confirmación indicando si se desea eliminar el documento
3. Elige[SI]	4. Elimina documento del usuario de la base de datos[firmas]
	5. Cumple con la meta: Auditar Eliminación de Documento.
	6. Elimina el documento de la bandeja de entrada.
	7. La meta MT27 finaliza.

Tabla 36. Descripción de la meta: Eliminar Bandeja de Entrada

Caso de Uso:	Gestionar Documentos Electrónicos	**Código Caso de Uso:**	CU08
Meta:	Crear un Borrador	**Código Meta:**	MT28
Propósito:	Crear un borrador		
Actor:	Administrador/Usuario		
Descripción:	El Administrador/usuario podrá crear un nuevo borrador, mismo que lo puede guardar para más tarde editarlo o eliminarlo.		
Referencia a requerimientos:	RF19		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador/usuario haya ingresado al sistema. • El administrador/usuario haya activado la página[Pag18: AdministrarDocumentos] sección Borradores		
Post condiciones:	• Editar Borrador • Eliminar Borrador. • Crear Borrador		

Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Elige la opción [Nuevo] del fragmento[FAdministrarDocumentos] de la página[Pag18:AdministrarDocumentos]	2. Muestra la página [Pag19:EditarDocumento]
3. Selecciona la categoría del documento en el fragmento[FNuevoDocumento] de la página[Pag19:EditarDocumento]	4. Carga la referencia correspondiente a la categoría seleccionada.
	5. Carga la plantilla que corresponde a la categoría seleccionada.
6. Ingresa el título del documento	7. Valida que se haya ingresado el título del documento.
8. Elige [Browser] o [Examinar] según el navegador.	9. Muestra un diálogo con el directorio a elegir para subir un archivo
10. Elige el archivo a subir	
11. Elige[Abrir] del cuadro de diálogo	12. Carga el archivo en el fragmento [FNuevoDocumento]
13. Elige[Subir]	14. Valida el tamaño del archivo a subir.
	15. Sube el archivo al servidor
	16. Muestra el nombre del archivo en el fragmento [FNuevoDocumento]
17. Ingresa el mensaje del documento.	18. Valida que se haya ingresado el mensaje del documento.
19. Ingresa el comentario del documento	
20. Elige [Guardar Borrador]	21. Guarda el borrador del usuario

	en la base de datos[firmas]
	22. La meta MT28 finaliza
Curso Alterno de Eventos	
Acción del actor	**Respuesta del sistema**
A. Campos requeridos	
	A.7. Presenta mensaje de validación indicando que el campo es requerido
	A.8. La meta continúa en el paso 6 del Curso Normal de Eventos
	A.18. Presenta mensaje de validación indicando que el campo es requerido
	A.19. La meta continúa en el paso 17 del Curso Normal de Eventos
B. Tamaño del archivo excede el rango permitido	
	B.14. Muestra un mensaje de validación indicando que el tamaño del archivo ha excedido el rango permitido.
	B.15. La meta continúa en el paso 8 del Curso Normal de Eventos.
C. Eliminar archivo adjunto	
C.17. Elige [Eliminar] en el fragmento [FNuevoDocumento]	C.18. Elimina el archivo del servidor
	C.19. Elimina el archivo del fragmento [FNuevoDocumento]
	C.20. La meta continúa en el paso 17 del Curso Normal de Eventos.

Tabla 37. Descripción de la meta: Crear un Borrador

Caso de Uso:	Gestionar Documentos Electrónicos	**Código Caso de Uso:**	CU08
Meta:	Editar un Borrador	**Código Meta:**	MT29
Propósito:	Editar un borrador		
Actor:	Administrador/Usuario		
Descripción:	El Administrador/usuario podrá editar un borrador que ya se encuentre almacenado en el sistema.		
Referencia a requerimientos:	RF19		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador/usuario haya ingresado al sistema. • El administrador/usuario haya activado la página[Pag18: AdministrarDocumentos], sección Borradores		
Post condiciones:	• Guardar Borrador		

	• Eliminar Borrador. • Crear Borrador
Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
1. Elige la opción [Editar] en uno de los borradores de la lista del fragmento[FAdministrarDocumentos] de la página[Pag18:AdministrarDocumentos]	2. Carga y muestra el borrador elegido en el fragmento [FNuevoDocumento] de la página [Pag19: EditarDocumento]
	3. La meta MT29 finaliza

Tabla 38. Descripción de la meta: Editar un Borrador

Caso de Uso:	Gestionar Documentos Electrónicos	**Código Caso de Uso:**	CU08
Meta:	Eliminar un Borrador	**Código Meta:**	MT30
Propósito:	Eliminar un borrador		
Actor:	Administrador/Usuario		
Descripción:	El Administrador/usuario podrá eliminar uno o varios borradores que se encuentren almacenados en el sistema, en la sección Borradores.		
Referencia a requerimientos:	RF19		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador/usuario haya ingresado al sistema. • El administrador/usuario haya activado la página[Pag18: AdministrarDocumentos], sección Borradores		
Post condiciones:	• Eliminar Borrador. • Crear Borrador. • Editar Borrador.		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige la opción [Eliminar] en uno de los borradores de la lista del fragmento[FAdministrarDocumentos] de la página[Pag18:AdministrarDocumentos]		2. Presenta un mensaje de confirmación indicando si se desea eliminar el borrador	
3. Elige [SI]		4. Elimina el borrador del usuario de la base de datos[firmas]	
		5. Elimina el borrador de la lista.	
		6. La meta MT30 finaliza	

Tabla 39. Descripción de la meta: Eliminar un Borrador

Caso de Uso:	Gestionar Documentos Electrónicos	**Código Caso de Uso:**	CU08
Meta:	Presentar Documentos	**Código Meta:**	MT31
Propósito:	Presentar documentos de la bandeja de entrada, salida, eliminados y borradores.		
Actor:	Administrador/Usuario		
Descripción:	El Administrador/usuario podrá visualizar los documentos con los que cuenta en la bandeja de entrada, salida, eliminados y borradores, dependiendo de su elección.		
Referencia a requerimientos:	RF17		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador/usuario haya ingresado al sistema. • El administrador/usuario haya activado la página[Pag18: AdministrarDocumentos]		
Post condiciones:	• Presentar Bandeja de Salida. • Presentar Documentos Eliminados. • Presentar Borradores		

Curso Normal de Eventos	
Acción del Actor	**Respuesta del Sistema**
	1. Obtener bandeja de entrada de documentos del usuario en la base de datos [firmas]
2. Selecciona el criterio para ordenar los documentos de la bandeja de entrada, en el fragmento [FAdministrarDocumentos] de la página[Pag18:AdministrarDocumentos]	3. Ordenar documentos de acuerdo al criterio elegido
	4. La meta MT31 finaliza

Curso Alterno de Eventos	
Acción del Actor	**Respuesta del Sistema**
A. Presentar bandeja de salida	
A.1. Selecciona la ficha [Bandeja de salida] en el fragmento [FAdministrarDocumentos] de la página[Pag18:AdministrarDocumentos]	A.2. Obtener bandeja de salida de documentos del usuario en la base de datos [firmas]
A.3. Selecciona el criterio para ordenar los documentos	A.4. Ordena los documentos de acuerdo al criterio elegido
	A.5. La meta MT31 finaliza
B. Presentar documentos eliminados	
B.1. Selecciona la ficha [Eliminados] en el fragmento[FAdministrarDocumentos] de la página[Pag18:AdministrarDocumentos]	B.2. Obtener documentos eliminados del usuario en la base de datos [firmas]
B.3. Selecciona el criterio para ordenar los documentos	B.4. Ordena los documentos de acuerdo al criterio elegido
	B.5. La meta MT31 finaliza

C. Presentar borradores	
C.1. Selecciona la ficha [Borradores] en el fragmento[FAdministrarDocumentos] de la página[Pag18:AdministrarDocumentos]	C.2. Obtener borradores del usuario en la base de datos [firmas]
C.3. Selecciona el criterio para ordenar los borradores	C.4. Ordena los documentos de acuerdo al criterio elegido
	C.5. La meta MT31 finaliza

Tabla 40. Descripción de la meta: Presentar Documentos

Caso de Uso:	Gestionar Documentos Electrónicos	**Código Caso de Uso:**	CU08
Meta:	Buscar Documentos	**Código Meta:**	MT32
Propósito:	Buscar documentos		
Actor:	Administrador		
Descripción:	El Administrador podrá visualizar la lista de todos los documentos que fueron enviados por los usuarios, para facilitar este proceso podrá elegir el criterio de búsqueda y en base a ello localizar de manera más rápida el documento buscado.		
Referencia a requerimientos:	RF16		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página [Pag03: Inicio]		
Post condiciones:	• Buscar Documentos		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige la opción [Documentos - Usuarios] del menú [Documentos] de la página [Pag03: Inicio]		2. Muestra la página[Pag20:Documentos]	
3. Elige el criterio de búsqueda en el fragmento[FDocumentos] de la página[Pag20:Documentos]			
4. Ingresa el texto correspondiente al correspondiente al criterio de búsqueda elegido.			
5. Elige[Buscar]		6. Presenta la lista de documentos encontrados en el fragmento[FDocumentos]	
		7. La meta MT32 finaliza.	

Tabla 41. Descripción de la meta: Buscar Documentos

Caso de Uso:	Generar Reportes	**Código Caso de Uso:**	CU09
Meta:	Generar Reportes	**Código Meta:**	MT33
Propósito:	Generar reportes de las acciones efectuadas en el sistema por los usuarios.		
Actor:	Administrador		
Descripción:	El Administrador podrá visualizar los reportes que el sistema genere en base a las acciones efectuadas en el mismo.		
Referencia a requerimientos:	RF28, RF29		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página [Pag03: Inicio]		
Post condiciones:	• Buscar Documentos		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige la opción [Reportes] del menú[Reportes] de la página [Pag03: Inicio]		2. Muestra y carga la lista de reportes disponibles en el fragmento[FReportes] de la página [Pag23: Reportes]	
3. Selecciona la fecha de inicio y finalización del reporte.		4. Valida que la fecha inicial no sea mayor a la final.	
		5. Valida que la fecha final no sea menor a la inicial	
6. Elige el reporte a visualizar		7. Genera y muestra el reporte en un archivo formato .pdf	
		8. La meta MT33 finaliza.	
Curso Alterno de Eventos			
A. Fecha inicial mayor a la final			
		A.4. Presenta un mensaje de validación indicando que la fecha inicial no puede ser mayor a la final	
		A.5. La meta continúa en el paso 3 del Curso Normal de Eventos.	
B. Fecha final menor a la inicial			
		B.5. Presenta un mensaje de validación indicando que la fecha final no puede ser menor a la inicial	
		B.6. La meta continúa en el paso 3 del Curso Normal de Eventos.	

Tabla 42. Descripción de la meta: Generar Reportes

Caso de Uso:	Generar Reportes	**Código Caso de Uso:**	CU09
Meta:	Ver Archivos Log's	**Código Meta:**	MT34
Propósito:	Visualizar archivos log's		
Actor:	Administrador		
Descripción:	El Administrador podrá visualizar los archivos log's que el sistema genere en base a las acciones efectuadas en el mismo.		
Referencia a requerimientos:	RF31		
Tipo de CU:	Primario		
Pre condiciones:	• El administrador haya ingresado al sistema. • El administrador haya activado la página [Pag24: Log]		
Post condiciones:	• Buscar Archivos Log's • Eliminar Archivos Log's		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
1. Elige la opción [Archivos de Log] del menú[Reportes] de la página [Pag03: Inicio]		2. Muestra la página [Pag24: Log]	
3. Selecciona fecha de inicio y finalización para visualizar archivos log's		4. Valida que la fecha inicial no sea mayor a la final.	
		5. Valida que la fecha final no sea menor a la inicial	
6. Elige [Buscar]		7. Muestra los log's encontrados.	
8. Elige [Ver] en unos de los archivos log presentados.		9. Muestra el archivo log elegido en la página [Pag25: VerLog]	
		10. La meta MT34 finaliza.	
Curso Alterno de Eventos			
A. Fecha Inicial mayor a la final			
		A.4. Presenta un mensaje de validación indicando que la fecha inicial no puede ser mayor a la final	
		A.5. La meta continúa en el paso 3 del Curso Normal de Eventos.	
B. Fecha final menor a la inicial			
		B.5. Presenta un mensaje de validación indicando que la fecha final no puede ser menor a la inicial	
		B.6. La meta continúa en el paso 3 del Curso Normal de Eventos.	
C. Eliminar archivo Log			
C.8. Elige [Eliminar] en unos de los archivos log's presentados en el fragmento[FLog] de la página [Pag24: Log]		C.9. Presenta mensaje de confirmación indicando si se desea eliminar el archivo log.	
C.10. Elige [Aceptar]		C.11. Elimina el archivo log seleccionado.	
		C.12. La meta MT34 finaliza	

Tabla 43. Descripción de la meta: Ver Archivos Log's

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Logeo	**Código Meta:**	MT35
Propósito:	Auditar logeo de un usuario		
Actor:	Sistema		
Descripción:	El Sistema auditará el logeo de un usuario.		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Iniciar Sesión		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene el usuario logeado	
		2. Genera auditoria del usuario logeado.	
		3. Guarda la auditoria	
		4. La meta MT035 finaliza.	

Tabla 44. Descripción de la meta: Auditar Logeo

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Creación de Usuario	**Código Meta:**	MT36
Propósito:	Auditar la creación de un usuario		
Actor:	Sistema		
Descripción:	El Sistema auditará la creación de un usuario.		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Crear Usuario.		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene el usuario creado.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria del usuario creado.	
		4. Guarda la auditoria.	
		5. La meta MT36 finaliza.	

Tabla 45. Descripción de la meta: Auditar Creación de Usuario

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Edición de Usuario.	**Código Meta:**	MT37
Propósito:	Auditar la edición de un usuario		
Actor:	Sistema		
Descripción:	El Sistema auditará la edición de un usuario.		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Editar Usuario.		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene el usuario editado.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria del usuario editado.	
		4. Guarda la auditoria	
		5. La meta MT37 finaliza.	

Tabla 46. Descripción de la meta: Auditar Edición de Usuario

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Eliminación de Usuario	**Código Meta:**	MT38
Propósito:	Auditar la eliminación de un usuario		
Actor:	Sistema		
Descripción:	El Sistema auditará la eliminación de un usuario.		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Eliminar Usuario.		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene el usuario eliminado.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria del usuario eliminado.	
		4. Guarda la auditoria	
		5. La meta MT38 finaliza.	

Tabla 47. Descripción de la meta: Auditar Eliminación de Usuario

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Creación de Certificado	**Código Meta:**	MT39
Propósito:	Auditar la creación de un certificado para un usuario.		
Actor:	Sistema		
Descripción:	El Sistema auditará la creación de un certificado digital.		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Crear Certificado		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene el certificado creado.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria del certificado creado.	
		4. Guarda la auditoria	
		5. La meta MT39 finaliza.	

Tabla 48. Descripción de la meta: Auditar Creación de Certificado

Caso de Uso:	Generar Reportes	**Código Caso de Uso:**	CU10
Meta:	Auditar Actualización de Certificado	**Código Meta:**	MT40
Propósito:	Auditar estado de un certificado.		
Actor:	Sistema		
Descripción:	El Sistema auditará la actualización del estado de un certificado digital.		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Dar de Baja a Certificado		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene el certificado actualizado.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria del certificado actualizado.	
		4. Guarda la auditoria	
		5. La meta MT40 finaliza.	

Tabla 49. Descripción de la meta: Auditar Actualización de Certificado

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Creación de Categoría	**Código Meta:**	MT41
Propósito:	Auditar creación de una categoría.		
Actor:	Sistema		
Descripción:	El Sistema auditará la creación de una categoría		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Crear Categoría		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene la categoría creada.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria de la categoría creada.	
		4. Guarda la auditoria	
		5. La meta MT41 finaliza.	

Tabla 50. Descripción de la meta: Auditar Creación de Categoría

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Edición de Categoría	**Código Meta:**	MT42
Propósito:	Auditar edición de una categoría.		
Actor:	Sistema		
Descripción:	El Sistema auditará la edición de una categoría		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Editar Categoría		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene la categoría editada.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria de la categoría editada.	
		4. Guarda la auditoria	
		5. La meta MT42 finaliza.	

Tabla 51. Descripción de la meta: Auditar Edición de Categoría

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Eliminación de Categoría	**Código Meta:**	MT43
Propósito:	Auditar eliminación de una categoría.		
Actor:	Sistema		
Descripción:	El Sistema auditará la eliminación de una categoría		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Eliminar Categoría		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene la categoría eliminada.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria de la categoría eliminada.	
		4. Guarda la auditoria	
		5. La meta MT43 finaliza.	

Tabla 52. Descripción de la meta: Auditar Eliminación de Categoría

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Creación de Plantilla	**Código Meta:**	MT44
Propósito:	Auditar creación de una plantilla		
Actor:	Sistema		
Descripción:	El Sistema auditará la creación de una plantilla		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Crear Plantilla		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene la plantilla creada	
		2. Obtiene el usuario logeado	
		3. Genera auditoria de la plantilla creada.	
		4. Guarda la auditoria	
		5. La meta MT44 finaliza.	

Tabla 53. Descripción de la meta: Auditar Creación de Plantilla

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Edición de Plantilla	**Código Meta:**	MT45
Propósito:	Auditar edición de una plantilla		
Actor:	Sistema		
Descripción:	El Sistema auditará la edición de una categoría		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Editar Plantilla		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene la plantilla editada.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria de la plantilla editada.	
		4. Guarda la auditoria	
		5. La meta MT45 finaliza.	

Tabla 54. Descripción de la meta: Auditar Edición de Plantilla

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Eliminación de Plantilla	**Código Meta:**	MT46
Propósito:	Auditar eliminación de una plantilla		
Actor:	Sistema		
Descripción:	El Sistema auditará la eliminación de una plantilla		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Eliminar Plantilla		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene la plantilla eliminada.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria de la plantilla eliminada.	
		4. Guarda la auditoria	
		5. La meta MT46 finaliza.	

Tabla 55. Descripción de la meta: Auditar Eliminación de Plantilla

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Creación de Departamento	**Código Meta:**	MT47
Propósito:	Auditar creación de un departamento.		
Actor:	Sistema		
Descripción:	El Sistema auditará la creación de un departamento.		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Crear Departamento		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene el departamento creado.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria del departamento creado.	
		4. Guarda la auditoria	
		5. La meta MT47 finaliza.	

Tabla 56. Descripción de la meta: Auditar Creación de Departamento

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Edición de Departamento	**Código Meta:**	MT48
Propósito:	Auditar edición de un departamento.		
Actor:	Sistema		
Descripción:	El Sistema auditará la edición de un departamento.		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Editar Departamento		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene el departamento editado.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria del departamento editado.	
		4. Guarda la auditoria	
		5. La meta MT48 finaliza.	

Tabla 57. Descripción de la meta: Auditar Edición de Departamento

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Eliminación de Departamento	**Código Meta:**	MT49
Propósito:	Auditar eliminación de un departamento.		
Actor:	Sistema		
Descripción:	El Sistema auditará la eliminación de un departamento.		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Eliminar Departamento		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene el departamento eliminado.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria del departamento eliminado.	
		4. Guarda la auditoria	
		5. La meta MT49 finaliza.	

Tabla 58. Descripción de la meta: Auditar Eliminación de Departamento

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Edición de Parámetro	**Código Meta:**	MT50
Propósito:	Auditar edición de parámetros		
Actor:	Sistema		
Descripción:	El Sistema auditará la edición de parámetros.		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Editar Parámetro		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		6. Obtiene el parámetro editado.	
		7. Obtiene el usuario logeado	
		8. Genera auditoria del parámetro editado.	
		9. Guarda la auditoria	
		10. La meta MT50 finaliza.	

Tabla 59. Descripción de la meta: Auditar Edición de Parámetro

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Auditar Creación de Documento	**Código Meta:**	MT51
Propósito:	Auditar creación de un documento.		
Actor:	Sistema		
Descripción:	El Sistema auditará la creación de un documento.		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Crear/Enviar Documento		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene el documento creado.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria del documento creado.	
		4. Guarda la auditoria	
		5. La meta MT51 finaliza.	

Tabla 60. Descripción de la meta: Auditar Creación de Documento

Caso de Uso:	Generar Reportes	**Código Caso de Uso:**	CU10
Meta:	Auditar Eliminación de Documento.	**Código Meta:**	MT52
Propósito:	Auditar eliminación de un documento.		
Actor:	Sistema		
Descripción:	El Sistema auditará la eliminación de un documento.		
Referencia a requerimientos:	RF30		
Tipo de CU:	Primario		
Pre condiciones:	Cumplimiento de la meta: Eliminar Bandeja de Entrada.		
Post condiciones:	Generar Reportes		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. Obtiene el documento eliminado por el usuario.	
		2. Obtiene el usuario logeado	
		3. Genera auditoria del documento eliminado.	
		4. Guarda la auditoria	
		5. La meta MT52 finaliza.	

Tabla 61. Descripción de la meta: Auditar Eliminación de Documento

Caso de Uso:	Efectuar Auditoría	**Código Caso de Uso:**	CU10
Meta:	Generar Archivos Log's	**Código Meta:**	MT53
Propósito:	Generar log's distribuidos en archivos info, warm, debug, error, fatal, trace para seguimiento de la aplicación.		
Actor:	Sistema		
Descripción:	El Sistema generará log's distribuidos en archivos info, warm, debug, error, fatal, trace; con la finalidad de capturar las acciones efectuadas en el sistema por parte de los usuarios.		
Referencia a requerimientos:	RF31		
Tipo de CU:	Primario		
Curso Normal de Eventos			
Acción del Actor		**Respuesta del Sistema**	
		1. El sistema invoca a info, warm, debug, error, fatal, trace del servicio log enviándole el mensaje de información y si es necesario la excepción producida.	
		2. El sistema verifica si el servicio log tiene asociado un archivo de log	
		3. Crea el archivo de log usando el nombre de usuario y la fecha como parte del nombre y ruta.	
		4. Formatea el mensaje de acuerdo al tipo de información	
		5. Agrega y escribe el mensaje al contenido del archivo	
		6. Cierra el archivo de log.	
		7. La meta MT53 finaliza.	

Tabla 62. Descripción de la meta: Generar Archivos Log's

Caso de Uso:	Administrar Respaldos	**Código Caso de Uso:**	CU11
Meta:	Buscar Respaldo	**Código Meta:**	MT54
Propósito:	Buscar un respaldo existente		
Actor:	Administrador		
Descripción:	El administrador podrá buscar un respaldo creado con anterioridad, para luego restaurarlo o en su defecto eliminarlo.		
Referencia a requerimientos:	RF32		
Tipo de CU:	Primario		
Pre condiciones:	El administrador se encuentre en la página [Pag26: Respaldos]		
Post condiciones:	Qué exista por los menos un respaldo almacenado en el sistema.		

Curso Normal de Eventos	
1. Elige la opción [Respaldos] de la página [Pag03: Inicio]	2. Muestra el fragmento [FRespaldos] en la página [Pag26: Respaldos]
3. Selecciona la fecha de inicio y finalización del respaldo a buscar	4. Valida que la fecha inicial no sea mayor a la final.
	5. Valida que la fecha final no sea menor a la inicial
6. Elige la opción[Buscar]	7. Busca los respaldos existentes.
	8. Muestra la lista de respaldos disponibles.
	9. La meta MT54 finaliza.
Curso Alterno de Eventos	
A. Fecha Inicial mayor a la final	
	A.4. Presenta un mensaje de validación indicando que la fecha inicial no puede ser mayor a la final
	A.5. La meta continúa en el paso 3 del Curso Normal de Eventos.
B. Fecha final menor a la inicial	
	B.5. Presenta un mensaje de validación indicando que la fecha final no puede ser menor a la inicial
	B.6. La meta continúa en el paso 3 del Curso Normal de Eventos.

Tabla 63. Descripción de la meta: Buscar Respaldo

Caso de Uso:	Administrar Respaldos	**Código Caso de Uso:**	CU11
Meta:	Crear Respaldo	**Código Meta:**	MT55
Propósito:	Crear un respaldo automático o manual.		
Actor:	Administrador/Sistema		
Descripción:	El administrador podrá crear un respaldo en el momento que él desee, caso contrario el sistema se encargará de ejecutar el respaldo que ya se encuentra programado.		
Referencia a requerimientos:	RF32		
Tipo de CU:	Primario		
Pre condiciones:	El administrador se encuentre en la página [Pag26: Respaldos]		
Post condiciones:	Buscar Respaldo		
Curso Normal de Eventos			
1. Elige la opción [Respaldos] en la página [Pag03: Inicio]		2. Muestra el fragmento [FRespaldos] en la página [Pag26: Respaldos]	

3. Elige la opción[Crear Respaldo]	4. Muestra el diálogo [DialogoEspere]
5. Elige [Iniciar]	6. Crea las carpetas para archivos subidos e imágenes.
	7. Verifica si la fecha actual del sistema ha sobrepasado la fecha del próximo respaldo.
	8. Verificar si el último respaldo se ha realizado y que los días del último y próximo respaldo sean diferentes
	9. Busca el parámetro definido para la ruta del respaldo.
	10. Crea los archivos, imágenes y files.
	11. Muestra el diálogo [DialogoFin] indicando que se ha terminado de ejecutar el respaldo.
12. Elige [Aceptar]	13. Guarda el respaldo en la ruta determinada.
	14. La meta MT55 finaliza
Curso Alterno de Eventos	
A. Respaldo automático	
	A.1. Verifica si la fecha actual del sistema ha sobrepasado la fecha del próximo respaldo.
	A.2. Verifica si el último respaldo se ha realizado y que los días del último y próximo respaldo sean diferentes
	A.3. Busca el parámetro definido para la ruta del respaldo.
	A.4. Crea los archivos, imágenes y files.
	A.5. Guarda el respaldo en la ruta determinada.
	A.6. La meta MT55 finaliza

Tabla 64. Descripción de la meta: Crear Respaldo

Caso de Uso:	Administrar Respaldos	**Código Caso de Uso:**	CU11
Meta:	Restaurar Respaldo	**Código Meta:**	MT56
Propósito:	Restaurar un respaldo creado o generado con anterioridad.		
Actor:	Administrador		
Descripción:	El administrador podrá restaurar la información del sistema como base de datos, archivos subidos e imágenes a través de la restauración de un respaldo determinado que previamente haya elegido.		
Referencia a requerimientos:	RF32		
Tipo de CU:	Primario		
Pre condiciones:	El administrador se encuentre en la página [Pag26: Respaldos] Cumplimiento de la meta: Buscar Respaldo		
Post condiciones:	Qué exista por lo menos un respaldo en el sistema.		
Curso Normal de Eventos			
1. Elige la opción [Restaurar] en la página [Pag26: Respaldos]		2. Muestra el diálogo [RestaurarRespaldo]	
3. Elige [Iniciar]		4. Crea los files de la Base de datos, archivos subidos e imágenes.	
		5. Verifica si existe la base de datos y los files.	
		6. Restaura la base de datos	
		7. Restaura los archivos subidos	
		8. Restaura archivos de imagen.	
		9. Muestra el diálogo [Restaurar] indicando que se ha terminado de ejecutar el respaldo.	
10. Elige [Aceptar]		11. La meta MT56 finaliza	

Tabla 65. Descripción de la meta: Restaurar Respaldo

Caso de Uso:	Administrar Respaldos	**Código Caso de Uso:**	CU11
Meta:	Eliminar Respaldo	**Código Meta:**	MT57
Propósito:	Eliminar un respaldo creado o generado con anterioridad.		
Actor:	Administrador		
Descripción:	El administrador podrá eliminar la información del sistema como base de datos, archivos subidos e imágenes a través de la eliminación de un respaldo determinado que previamente haya elegido o buscado.		
Referencia a requerimientos:	RF32		
Tipo de CU:	Primario		

Pre condiciones:	El administrador se encuentre en la página [Pag26: Respaldos] Cumplimiento de la meta: Buscar Respaldo
Post condiciones:	Qué exista por lo menos un respaldo en el sistema.
Curso Normal de Eventos	
1. Elige la opción [Eliminar] en la página [Pag26: Respaldos]	2. Presenta mensaje de confirmación indicando si se desea eliminar el respaldo seleccionado..
3. Elige [Aceptar]	4. Elimina el respaldo seleccionado.
	5. La meta MT57 finaliza

Tabla 66. Descripción de la meta: Eliminar Respaldo

8.9. DIAGRAMAS DEL SISTEMA

8.9.1. DIAGRAMAS DE SECUENCIA

CASO DE USO CU01: LOGEAR USUARIOS

MT01: Iniciar Sesión

Curso Normal de Eventos

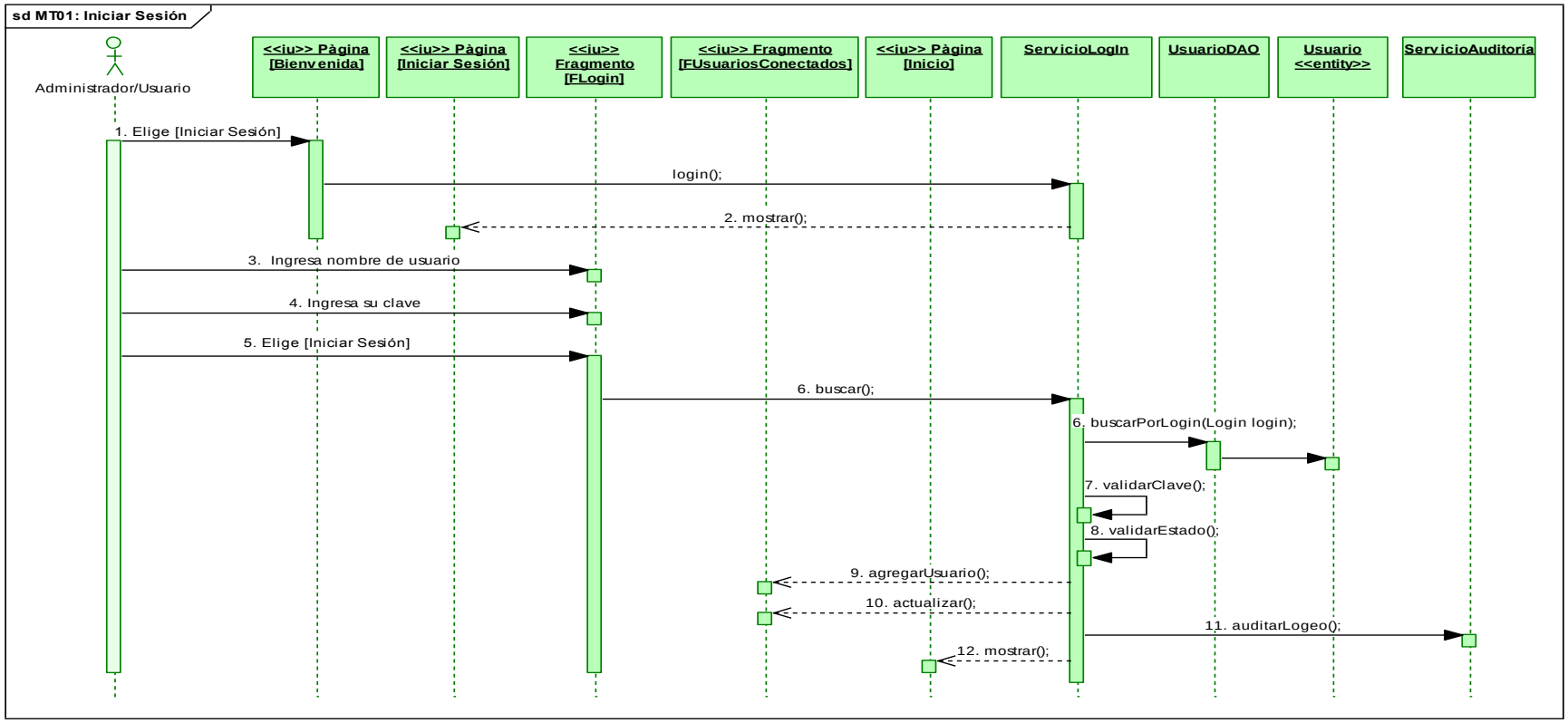


Fig.75. DS Curso Normal: Iniciar Sesión

Cursos Alternos de Eventos

A. Usuario no encontrado

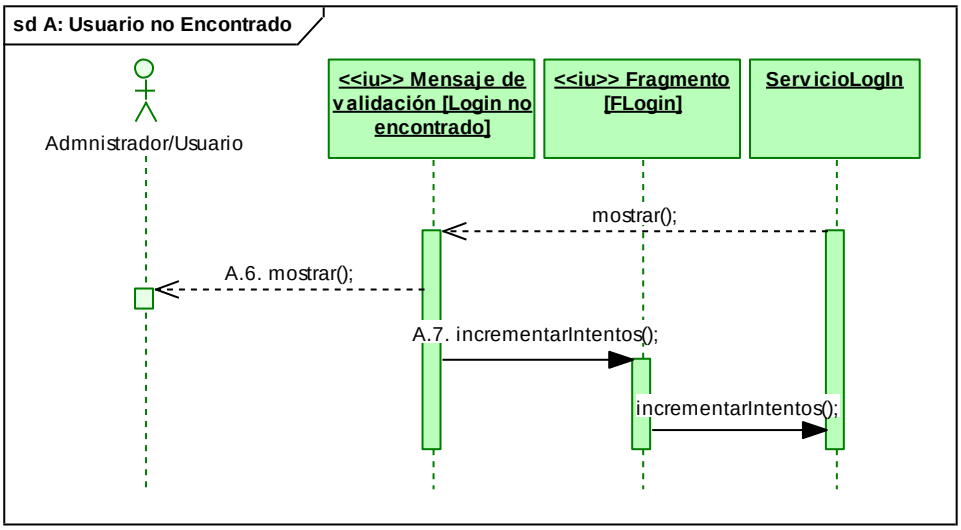


Fig.76. DS Curso Alterno: Usuario no encontrado

B. Clave Incorrecta

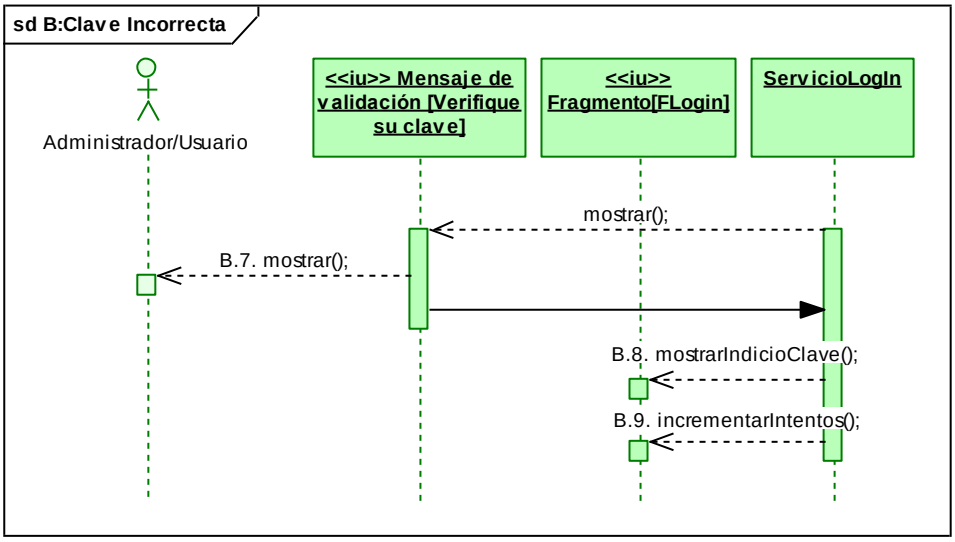


Fig.77. DS Curso Alterno: Clave Incorrecta

C. Número máximo de intentos sobrepasado

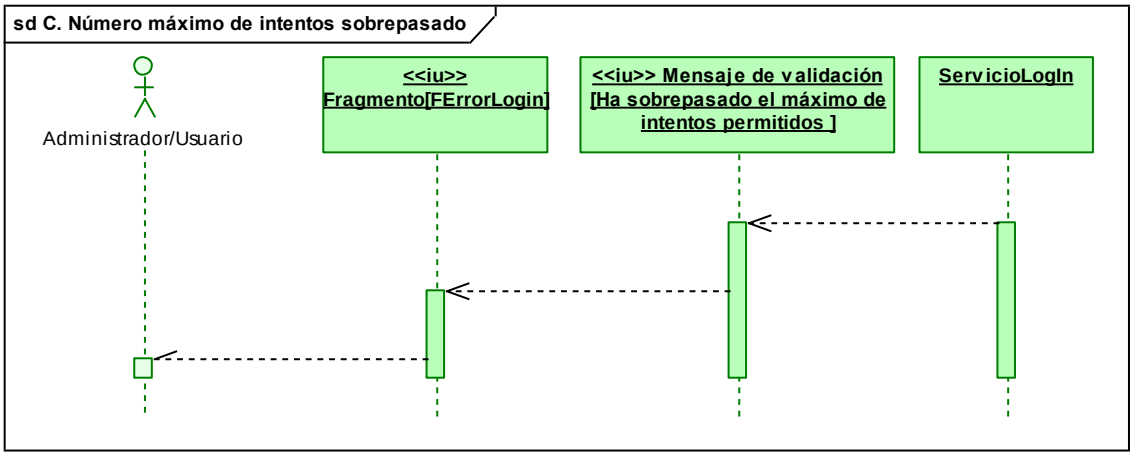


Fig.78. DS Curso Alterno: Número máximo de intentos sobrepasado

D. Usuario inactivo

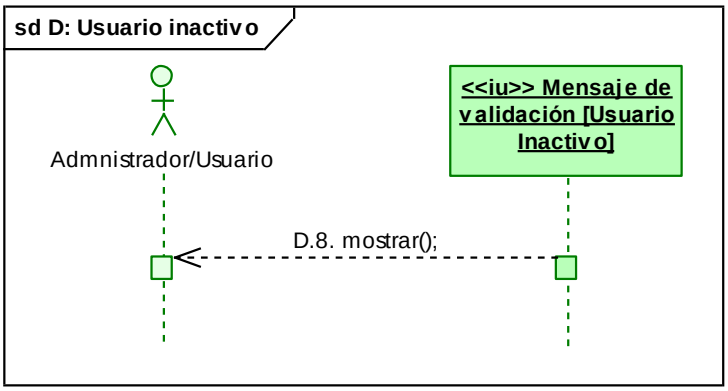


Fig.79. DS Curso Alterno: Usuario inactivo

MT02: Cerrar Sesión

Curso Normal de Eventos

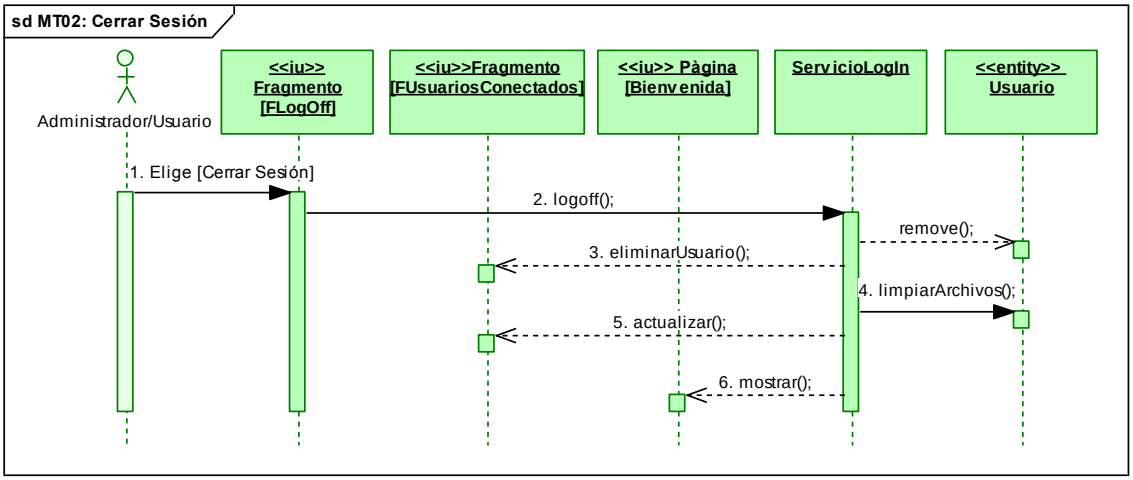


Fig.80. DS Curso Normal: Cerrar Sesión

Cursos Alternos de Eventos

A. Sesión expirada:

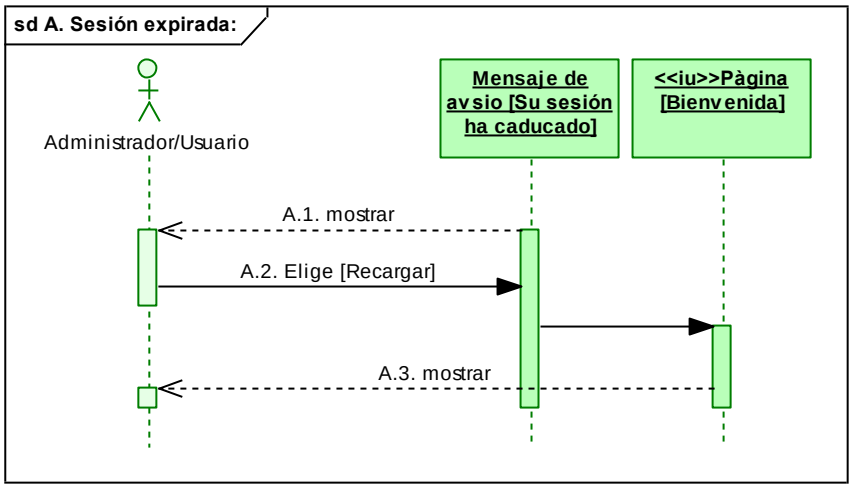


Fig.81. DS Curso Alterno: Sesión expirada

CASO DE USO CU02: ADMINISTRAR USUARIOS

MT03: Crear Usuario

Curso Normal de Eventos

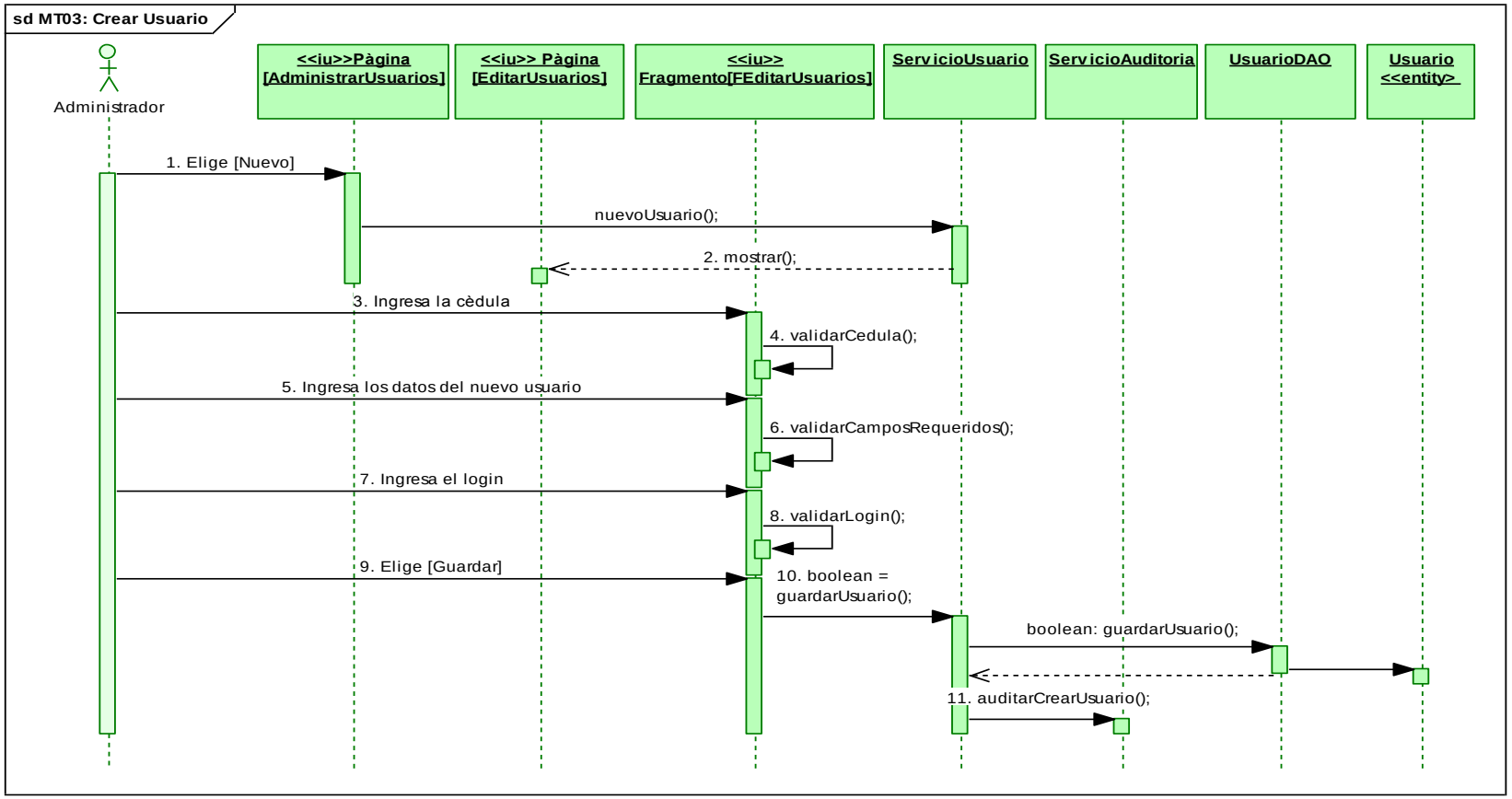


Fig.82. DS Curso Normal: Crear Usuario

Cursos Alternos de Eventos

A. Cedula Incorrecta

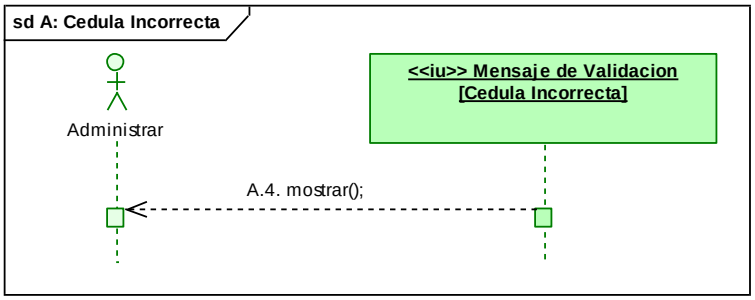


Fig.83. DS Curso Alterno: Cédula Incorrecta

B. Cedula Duplicada

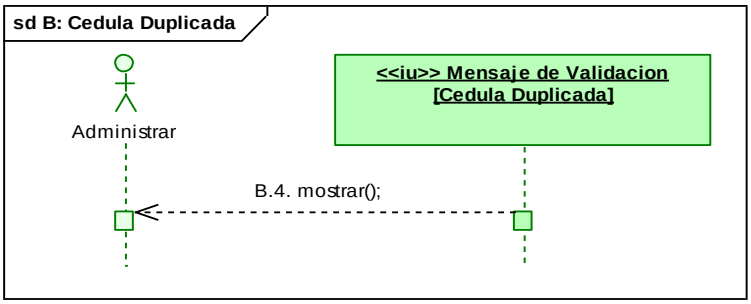


Fig.84. DS Curso Alterno: Cédula Duplicada

C. Campos Requeridos

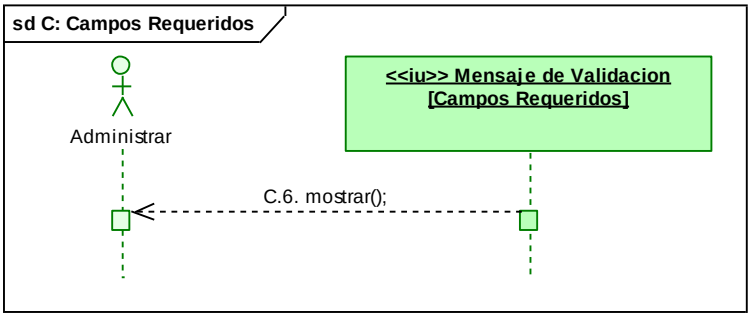


Fig.85. DS Curso Alterno: Campos Requeridos

D. Usuario Duplicado

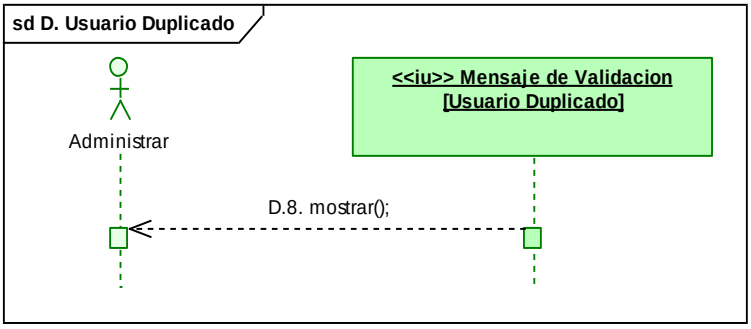


Fig.86. DS Curso Alterno: Usuario Duplicado

MT04: Buscar Usuario

Curso Normal de Eventos

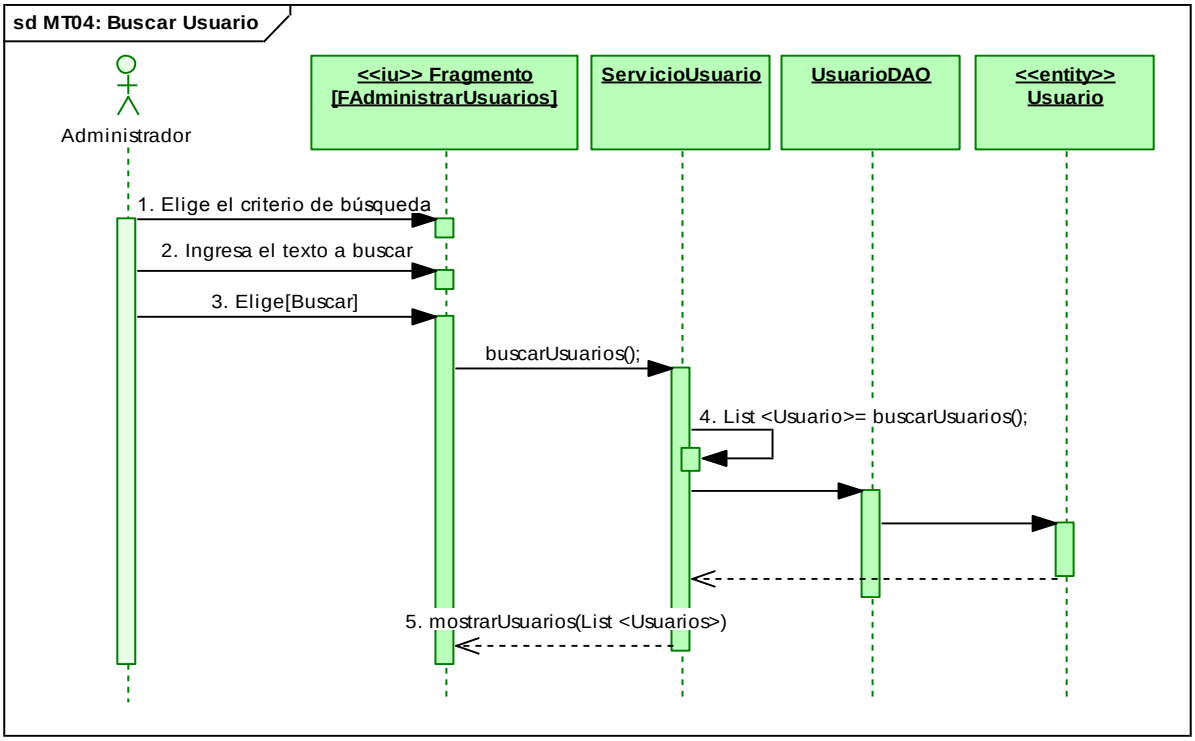


Fig.87. DS Curso Normal: Buscar Usuario

MT05: Editar Usuario

Curso Normal de Eventos

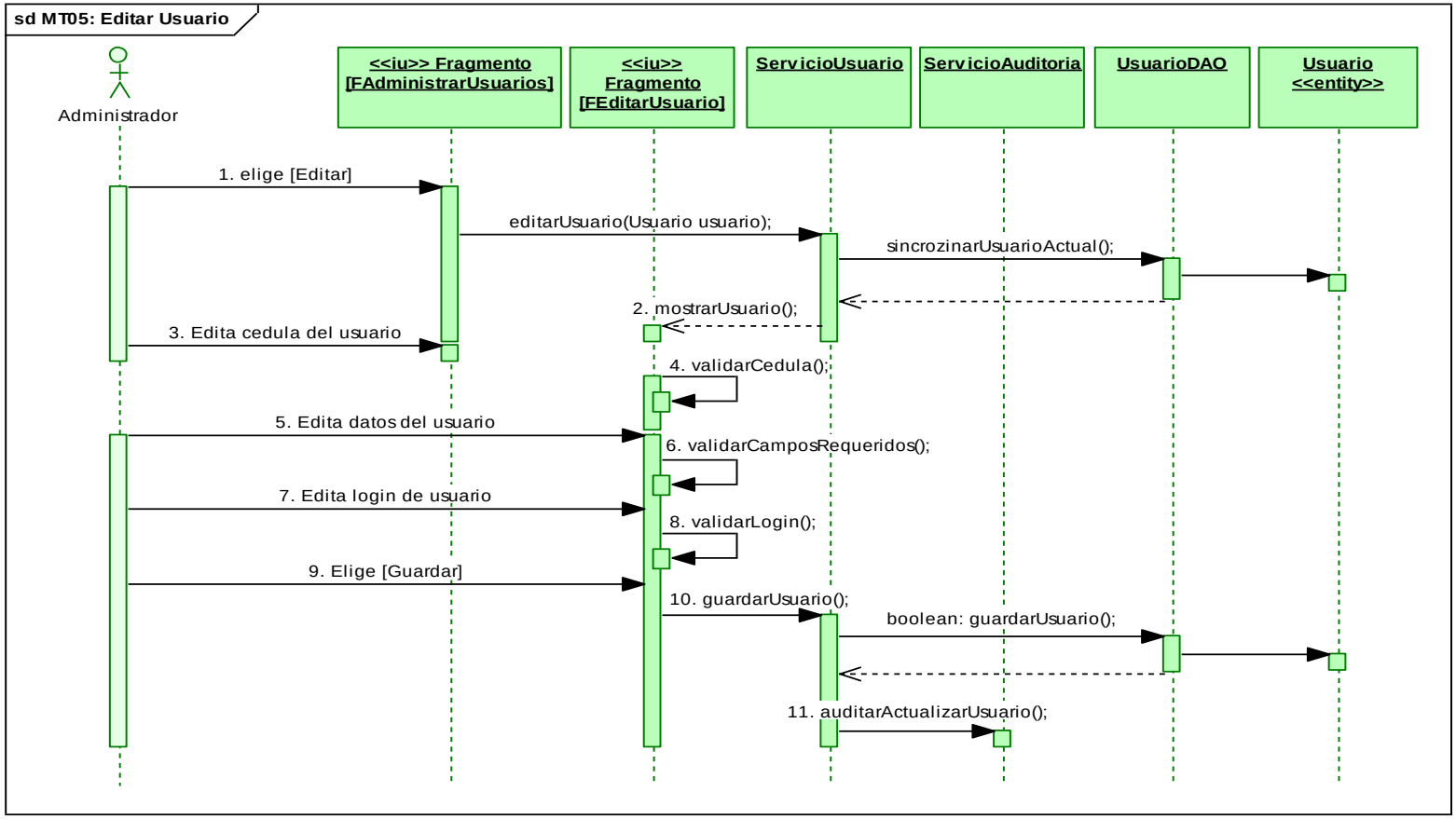


Fig.88. DS Curso Normal: Editar Usuario

Cursos Alternos de Eventos

A. Cambiar estado de usuario

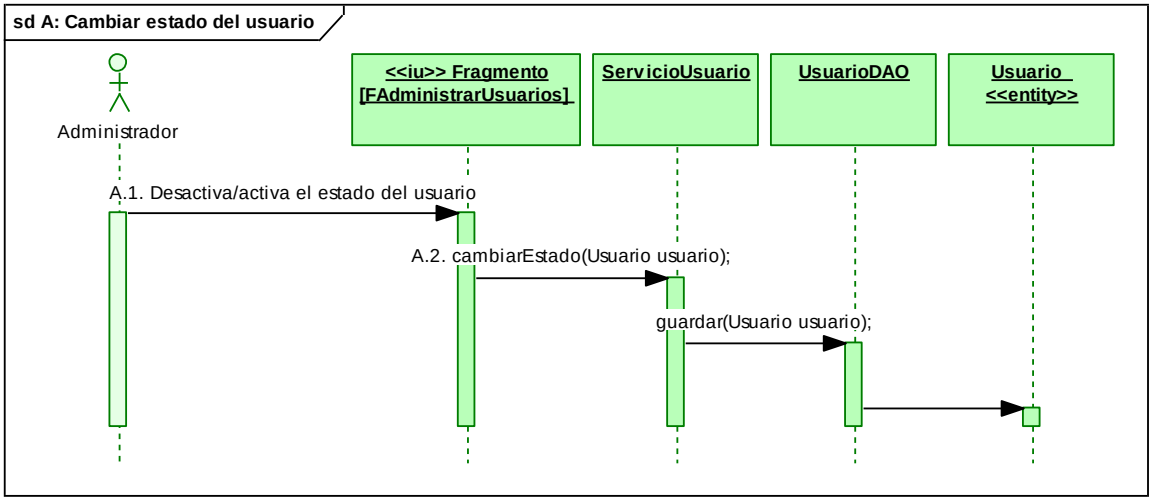


Fig.89. DS Curso Alterno: Cambiar estado de usuario

B. Resetear clave

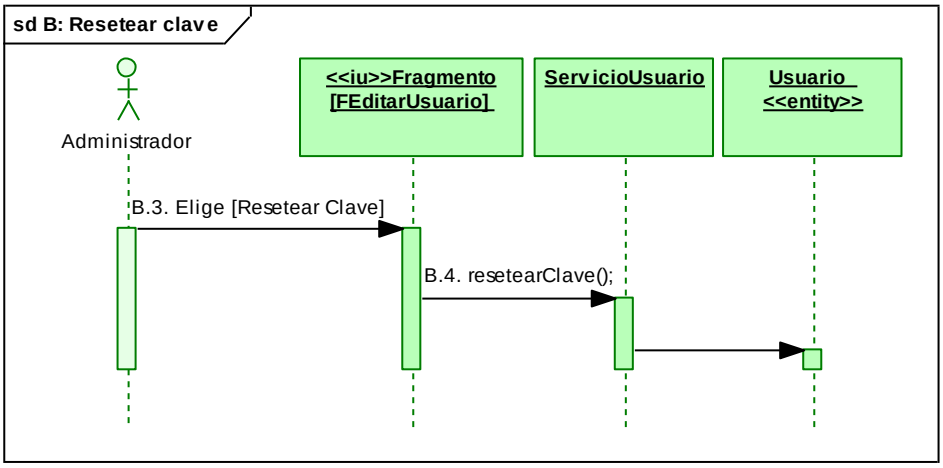


Fig.90. DS Curso Alterno: Resetear clave

C. Cédula Incorrecta

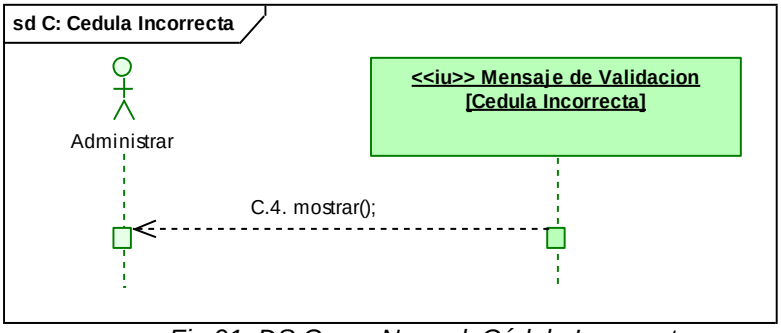


Fig.91. DS Curso Normal: Cédula Incorrecta

D. Cedula Duplicada

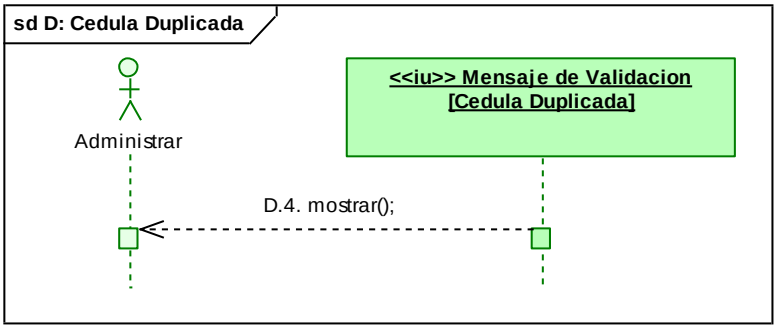


Fig.92. DS Curso Alterno. Cédula Duplicada

E. Campos Requeridos

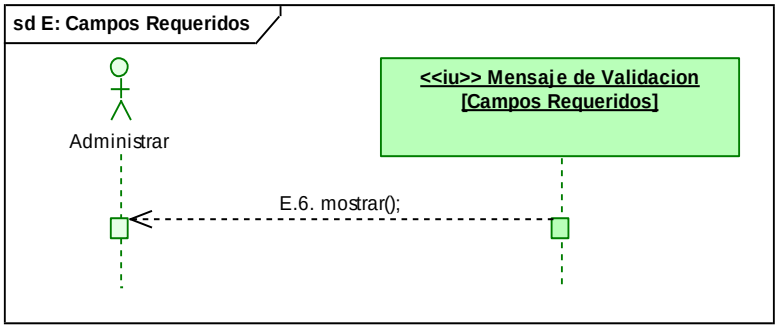


Fig.93. DS Curso Alterno: Campos Requeridos

F. Usuario Duplicado

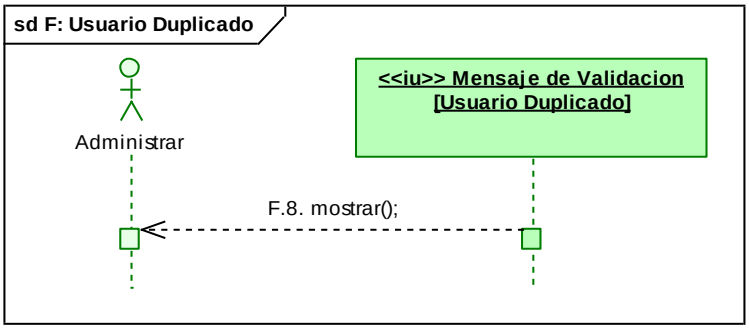


Fig.94. DS Curso Alterno: Usuario Duplicado

MT06: Cambiar Clave

Curso Normal de Eventos

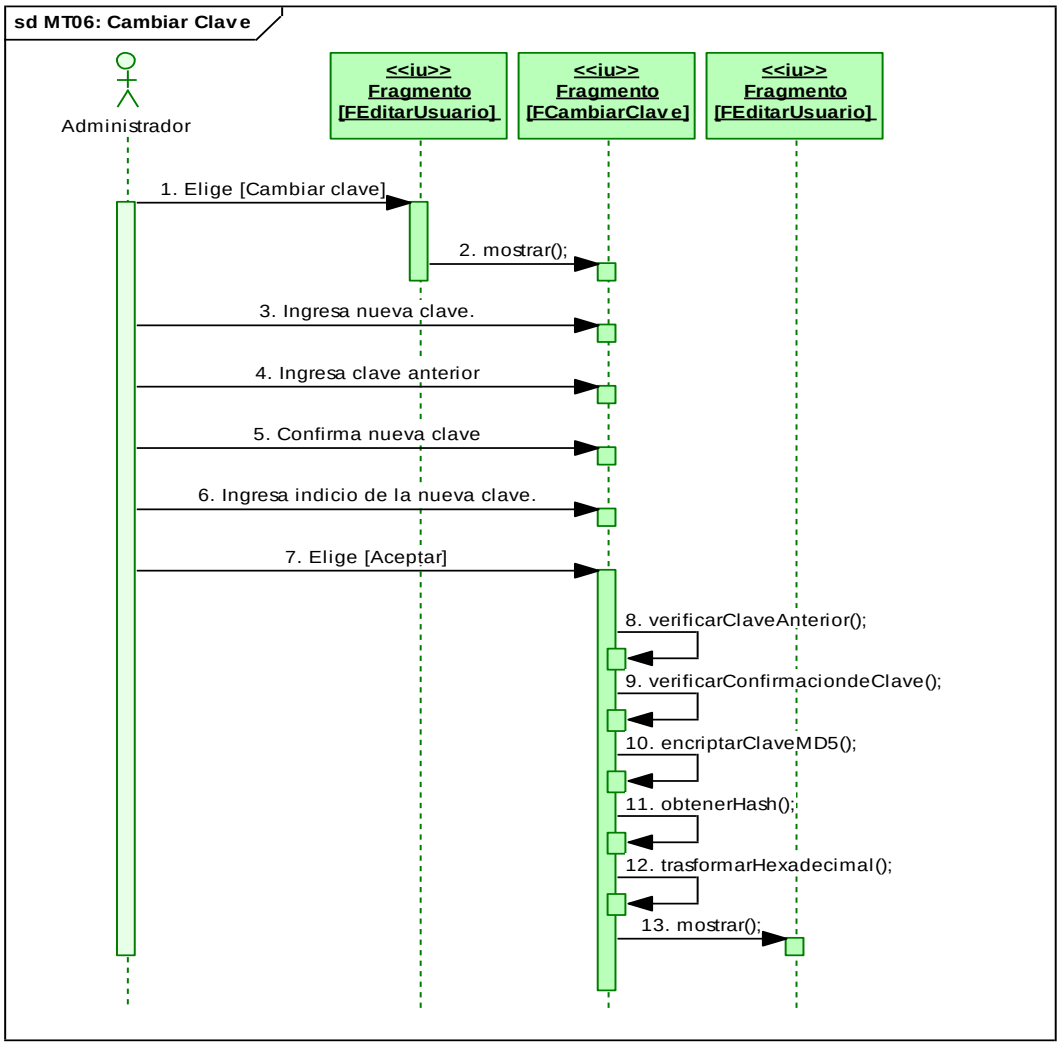


Fig.95. DS Curso Normal: Cambiar Clave

Cursos Alternos de Eventos

A. Clave anterior incorrecta

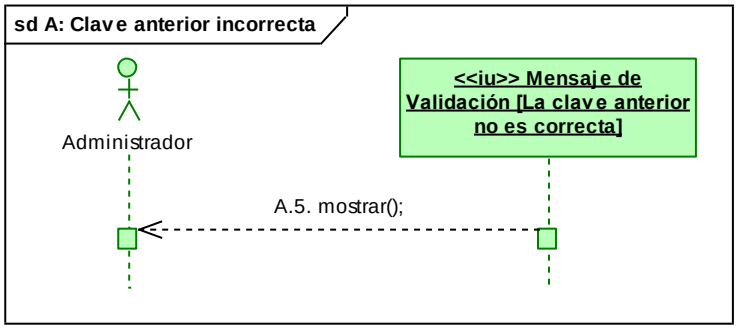


Fig.96. DS Curso Alterno: Clave anterior incorrecta

MT07: Eliminar Usuario

Curso Normal de Eventos

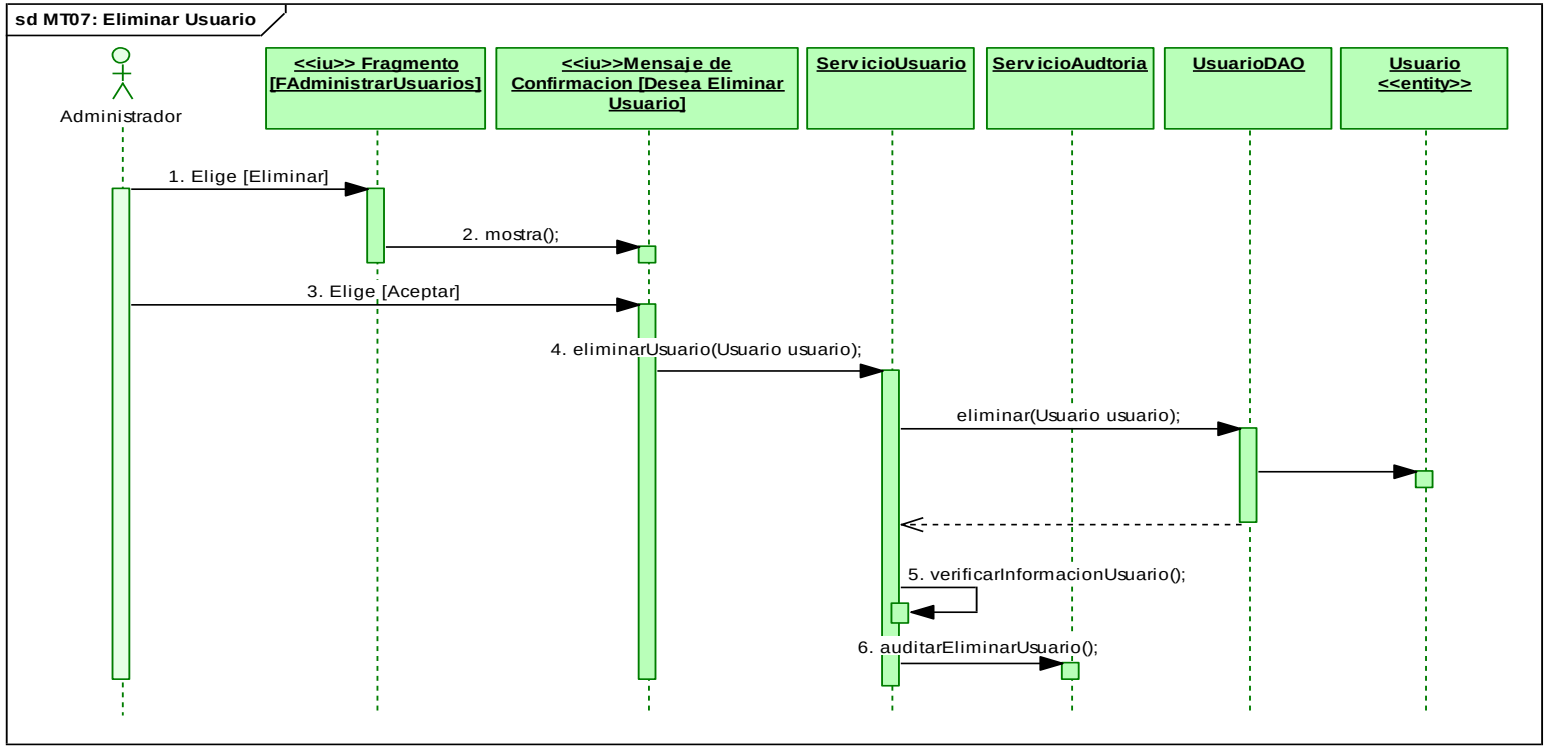


Fig.97. DS Curso Normal: Eliminar Usuario

MT08: Editar Perfil

Curso Normal de Eventos

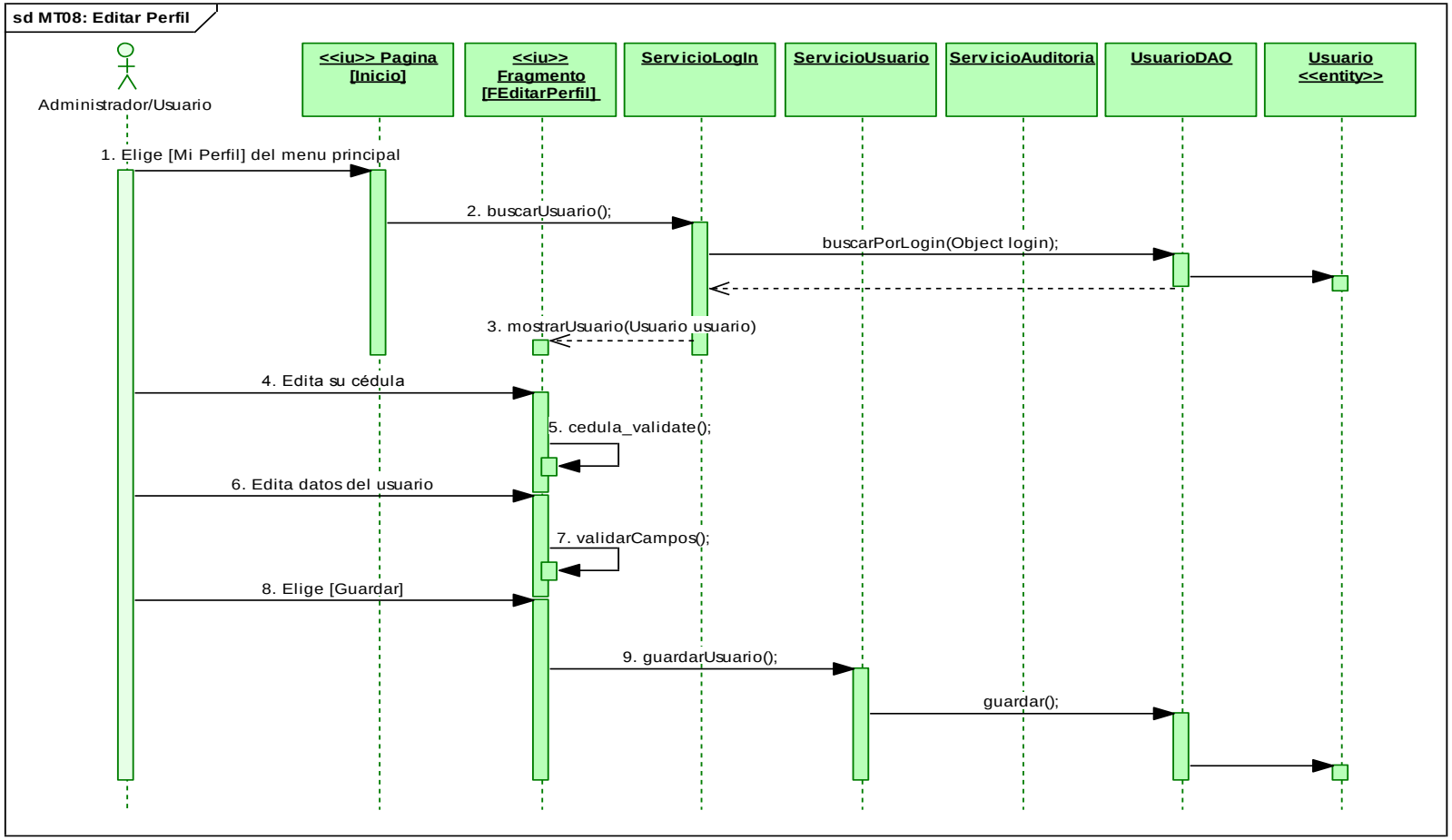


Fig.98. DS Curso Normal: Editar Perfil

Cursos Alternos de Eventos

A. Cédula Incorrecta

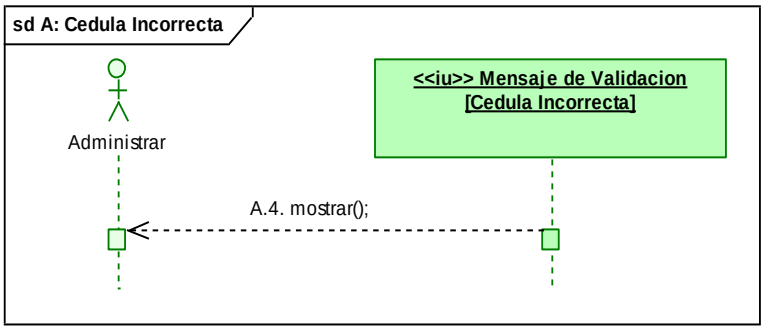


Fig.99. DS Curso Alterno: Cédula Incorrecta

B. Cédula Duplicada

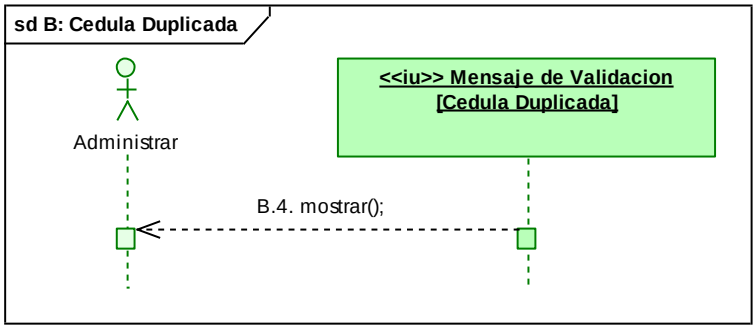


Fig.100. DS Curso Alterno: Cédula Duplicada

C. Campos Requeridos

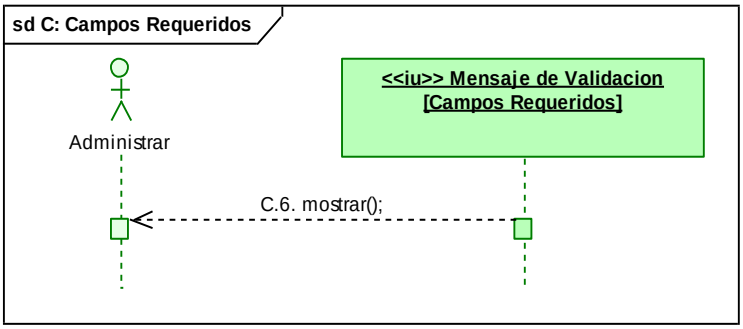


Fig.101. DS Curso Alterno: Campos Requeridos

CASO DE USO CU03: ADMINISTRAR CERTIFICADOS

MT09: Crear Certificado

Curso Normal de Eventos

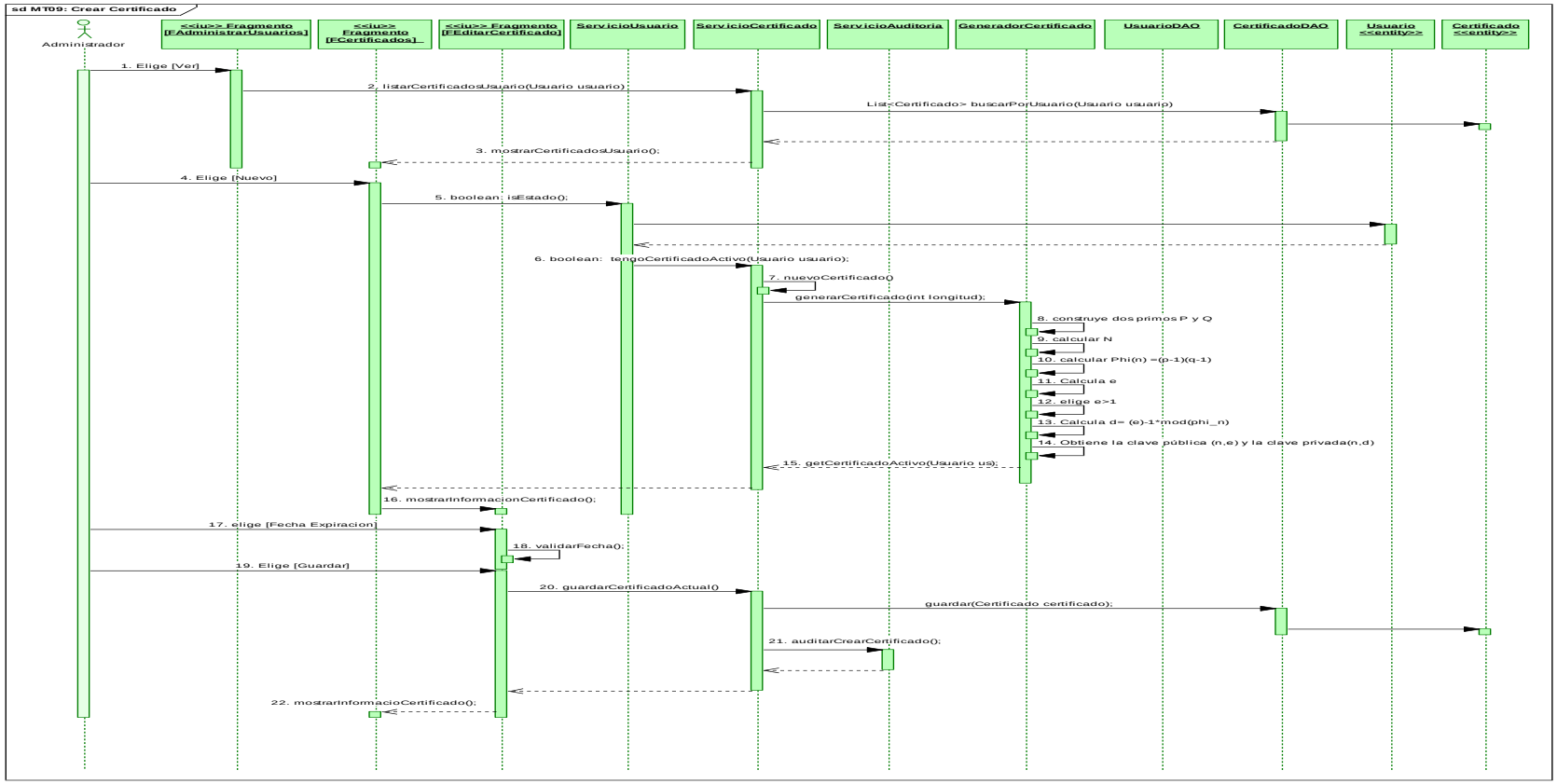


Fig.102. DS Curso Normal. Crear Certificado

Cursos Alternos de Eventos

A. Ver Certificado en PDF

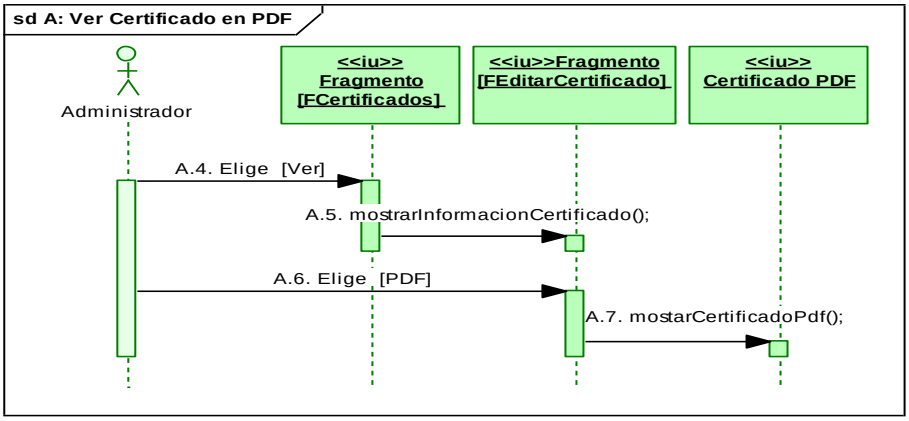


Fig.103. DS Curso Alterno: Ver Certificado en PDF

B. Guardar Claves

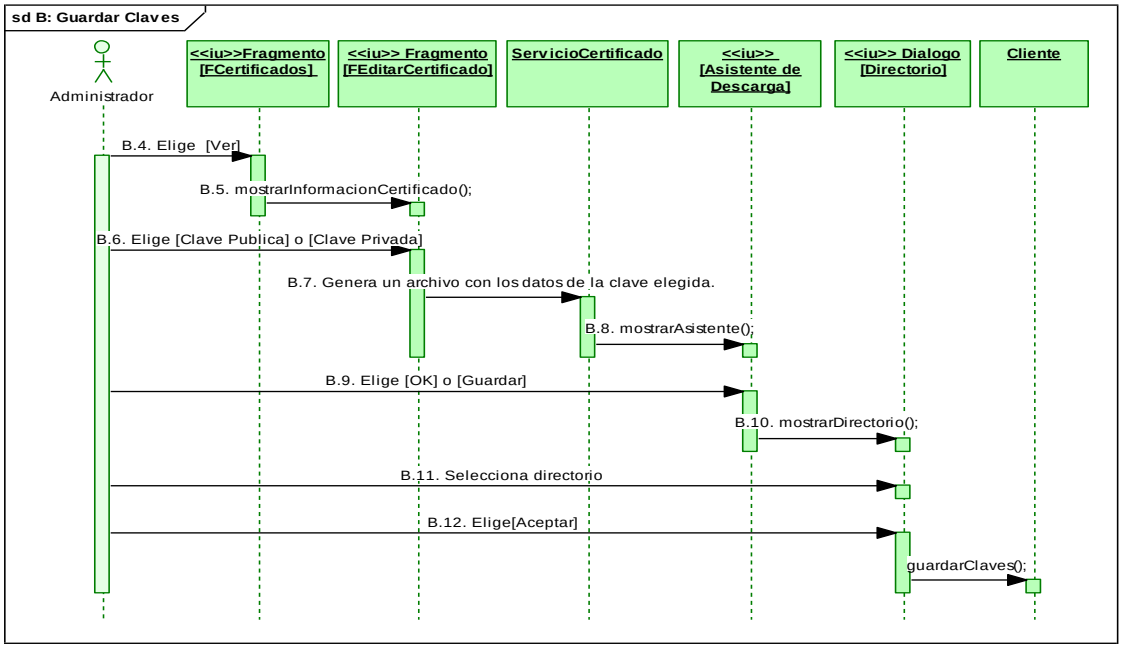


Fig.104. DS Curso Alterno: Guardar Claves

C. Usuario Inactivo

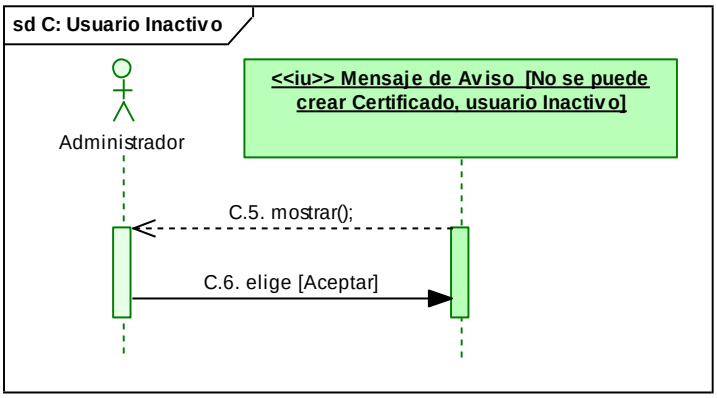


Fig.105. DS Curso Alterno: Usuario Inactivo

D. Nuevo certificado disponiendo de uno activo

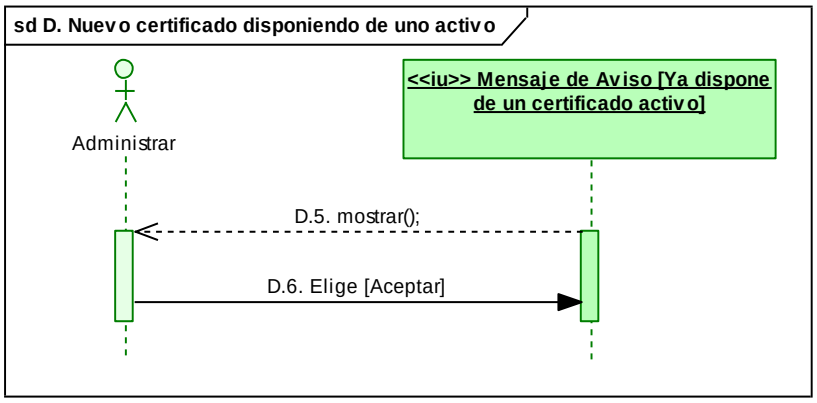


Fig.106. DS Curso Alterno: Nuevo certificado disponiendo de uno activo

E. Fecha de expiración igual a la de creación

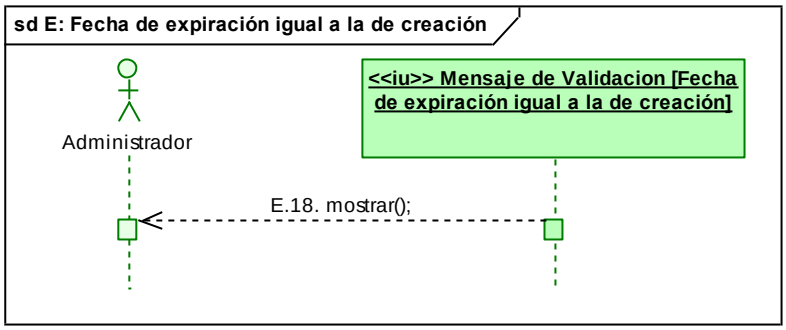


Fig.107. DS Curso Alterno: Fecha de expiración igual a la de creación

MT10: Dar de Baja Certificado

Curso Normal de Eventos

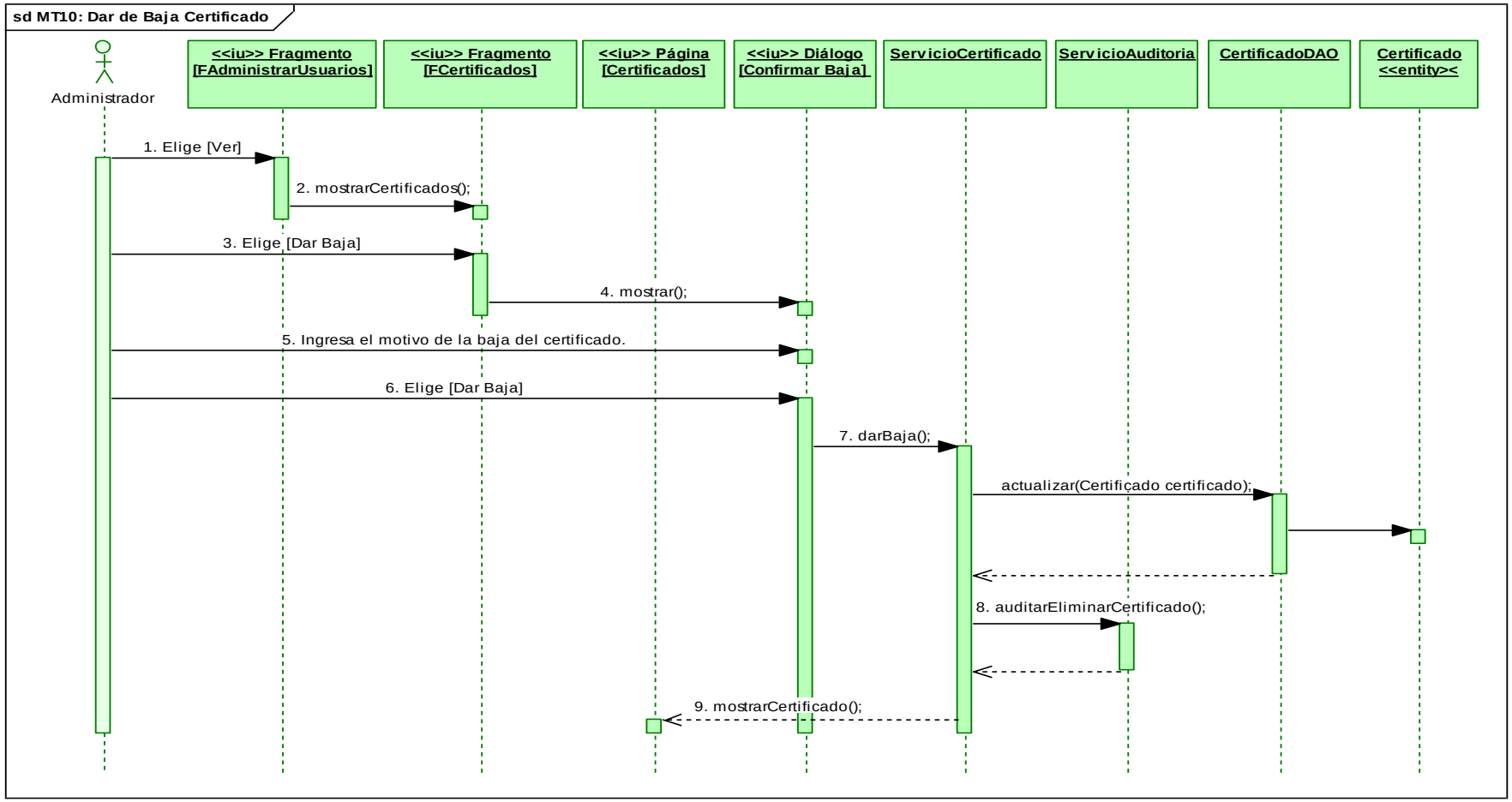


Fig.108. DS Curso Normal: Dar de baja Certificado

CASO DE USO CU04: ADMINISTRAR CATEGORÍAS

MT11: Crear Categoría

Curso Normal de Eventos

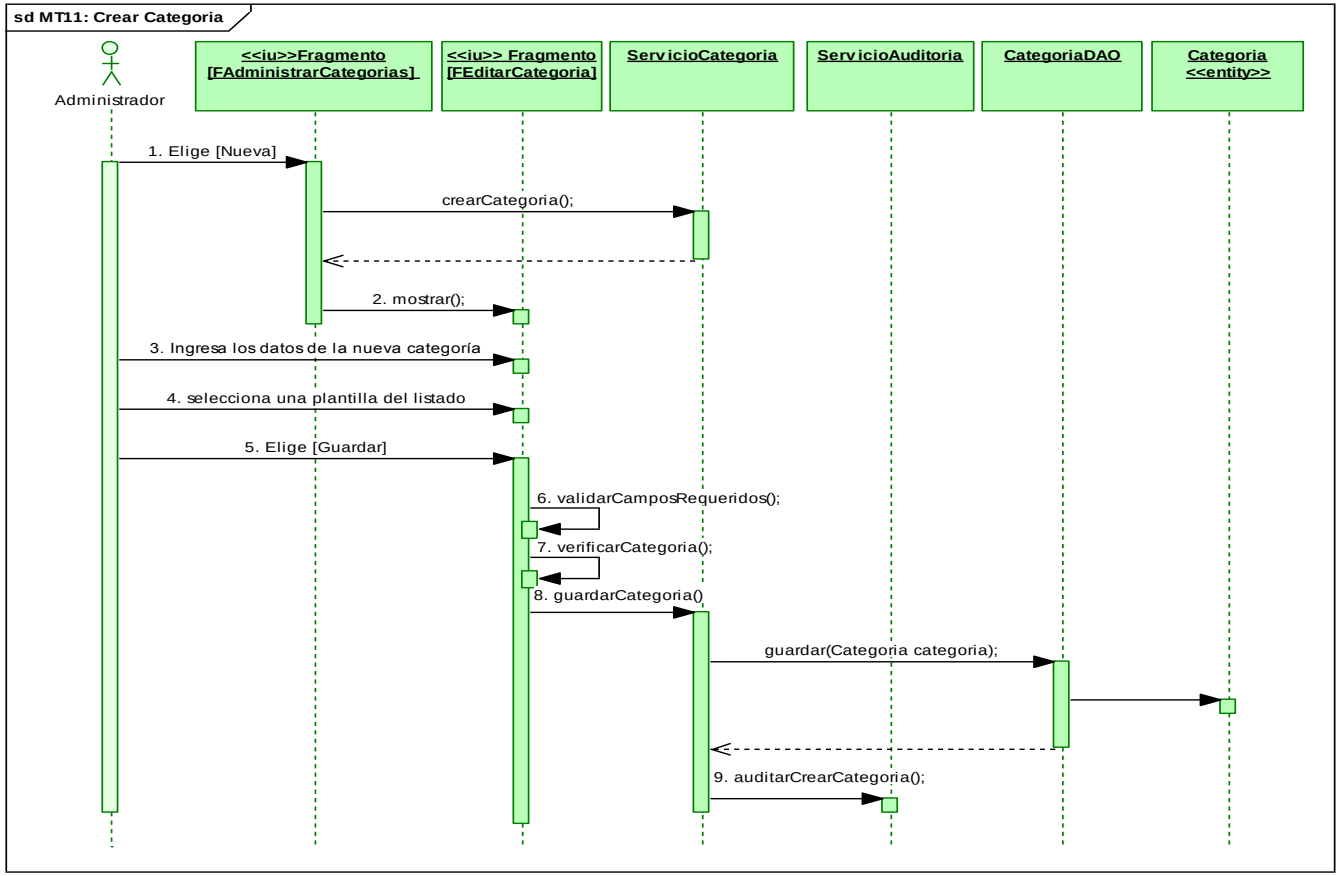


Fig.109. DS Curso Normal: Crear Categoría

Cursos Alternos de Eventos

A. Campos requeridos

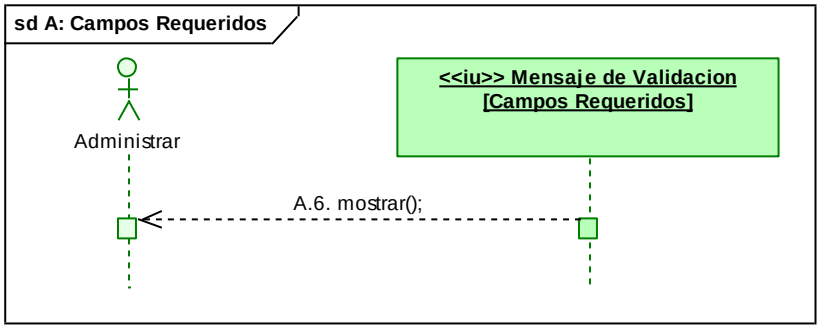


Fig.110. DS Curso Alterno: Campos Requeridos

B. Nombre de categoría duplicada

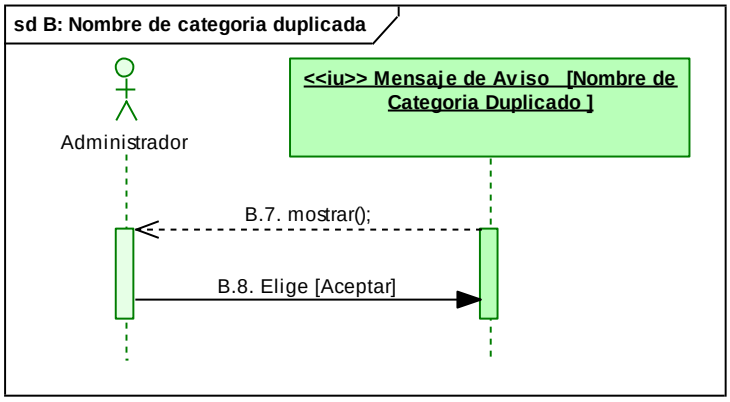


Fig.111. DS Curso Alterno: Nombre de categoría duplicada

MT12: Editar Categoría

Curso Normal de Eventos

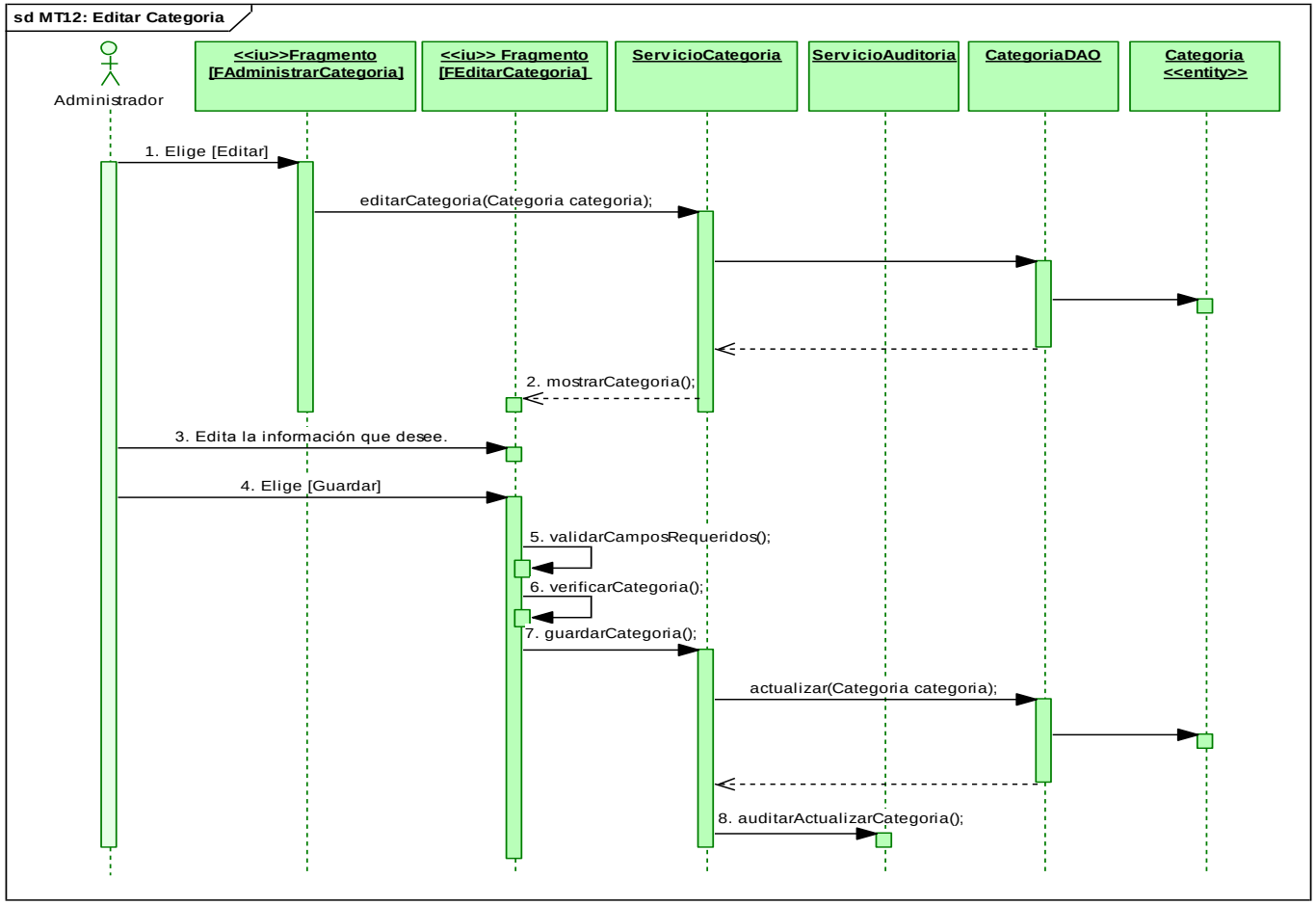


Fig.112. DS Normal: Editar Categoría

Cursos Alternos de Eventos

A. Campos Requeridos

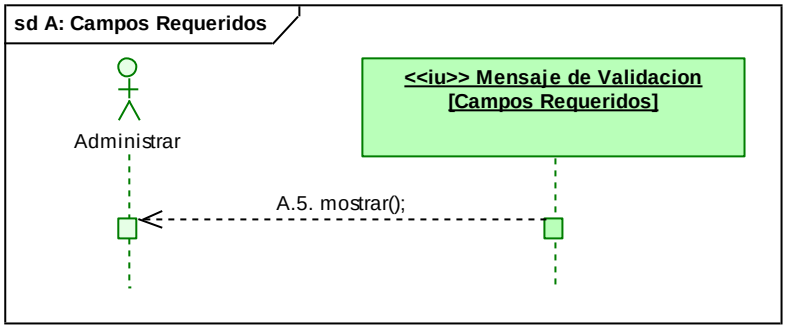


Fig.113. DS Curso Alterno: Campos Requeridos

B. Nombre de categoría duplicada

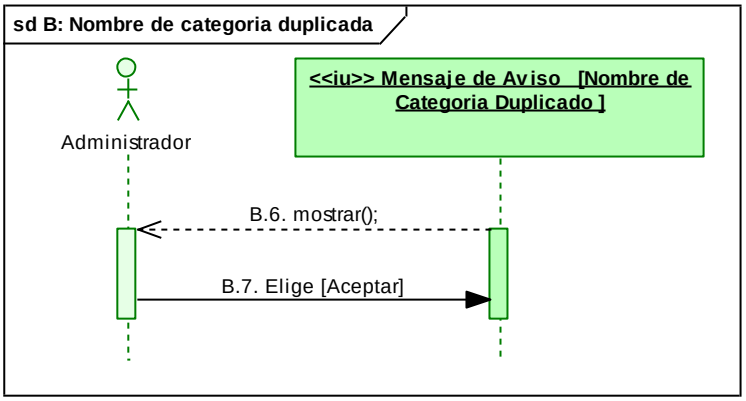


Fig.114. DS Curso Alterno: Nombre de categoría duplicada

MT13: Eliminar Categoría

Curso Normal de Eventos

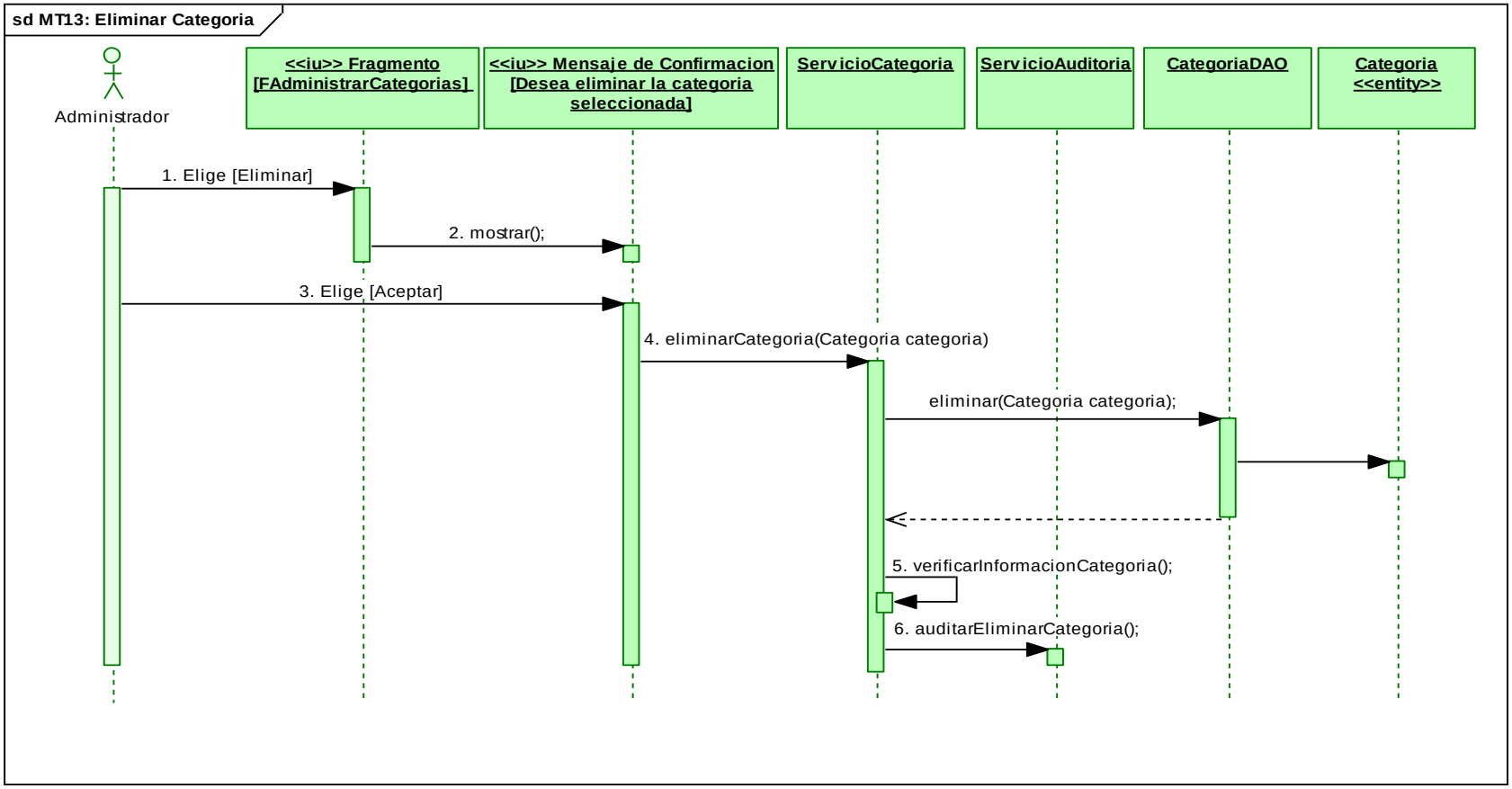


Fig.115. DS Curso Normal. Eliminar Categoría

CASO DE USO CU05: ADMINISTRAR PLANTILLAS

MT14: Crear Plantilla

Curso Normal de Eventos

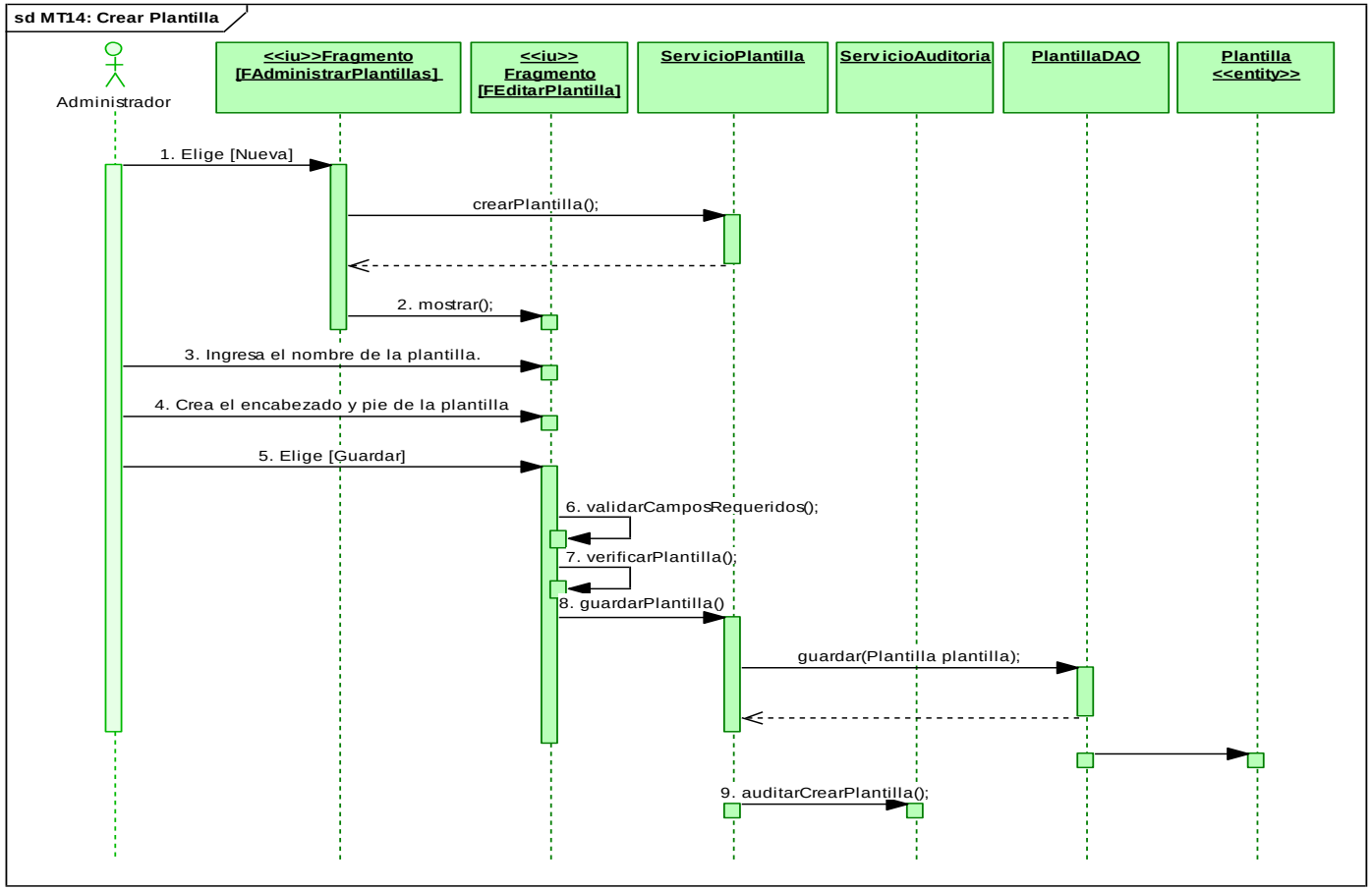


Fig.116. DS Curso Normal. Crear Plantilla

Cursos Alterno de Eventos

A. Crear plantilla a partir de las opciones de [Ayuda]

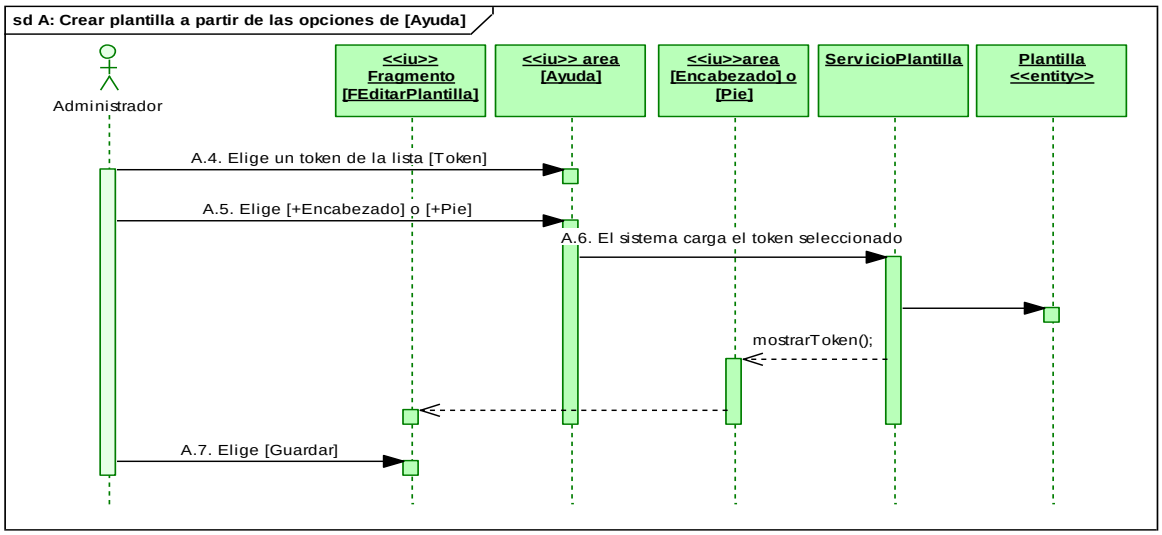


Fig.117. DS Curso Alterno: Crear plantilla a partir de las opciones de [Ayuda]

B. Campos Requeridos

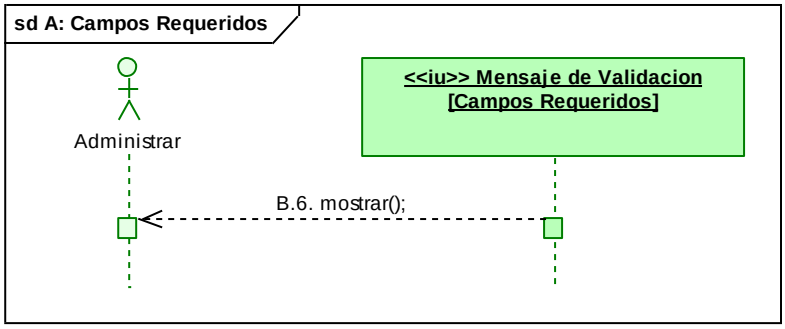


Fig.118. DS Curso Alterno: Campos Requeridos

C. Nombre de plantilla duplicada

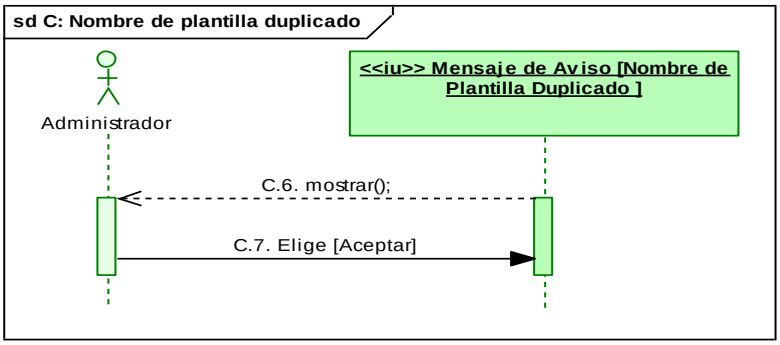


Fig.119. DS Curso Alterno: Nombre de plantilla duplicado

MT15: Editar Plantilla

Curso Normal de Eventos

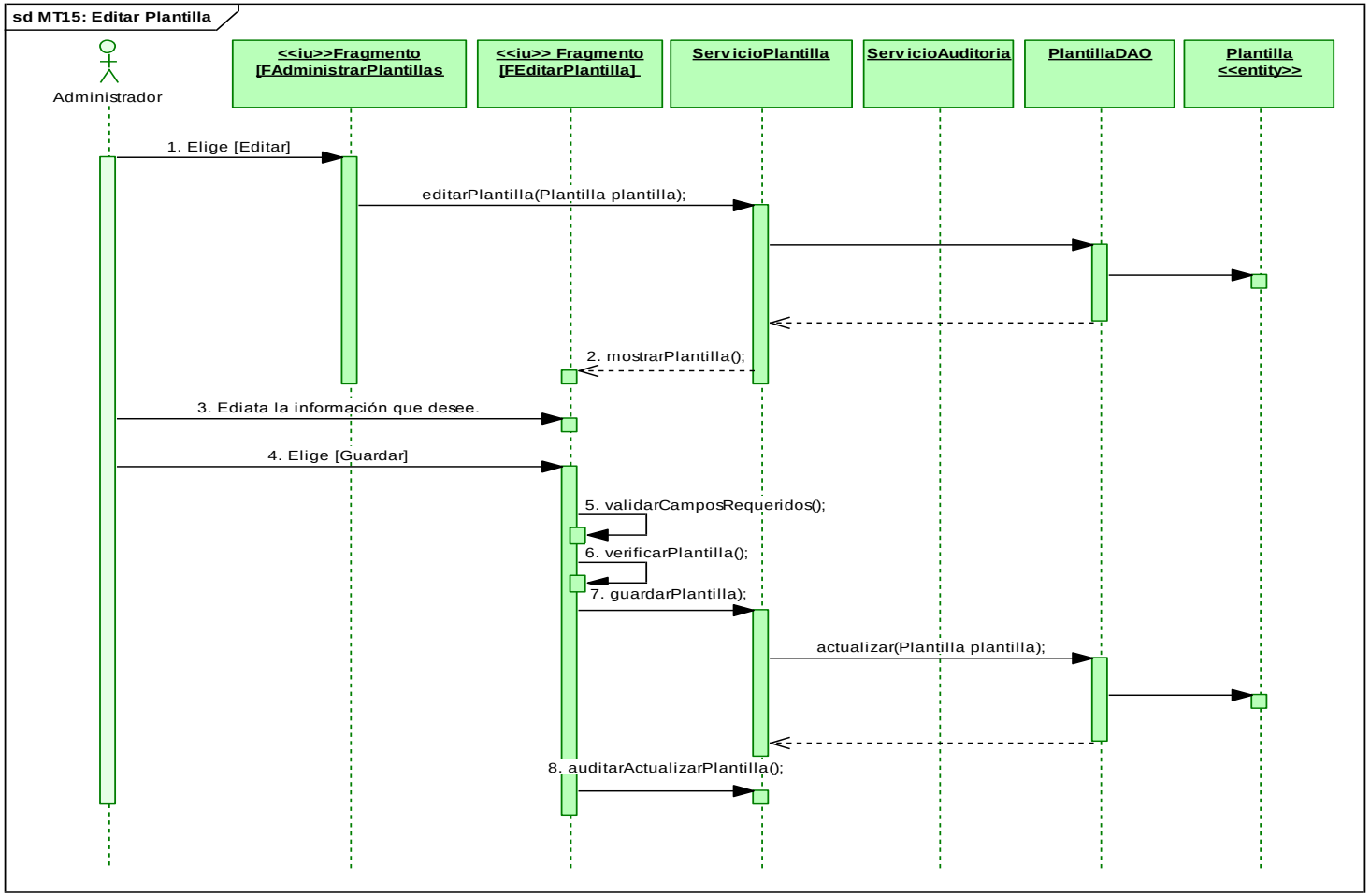


Fig.120. DS Curso Normal: Editar Plantilla

Curso Alterno de Eventos

A. Editar plantilla a partir de las opciones de [Ayuda]

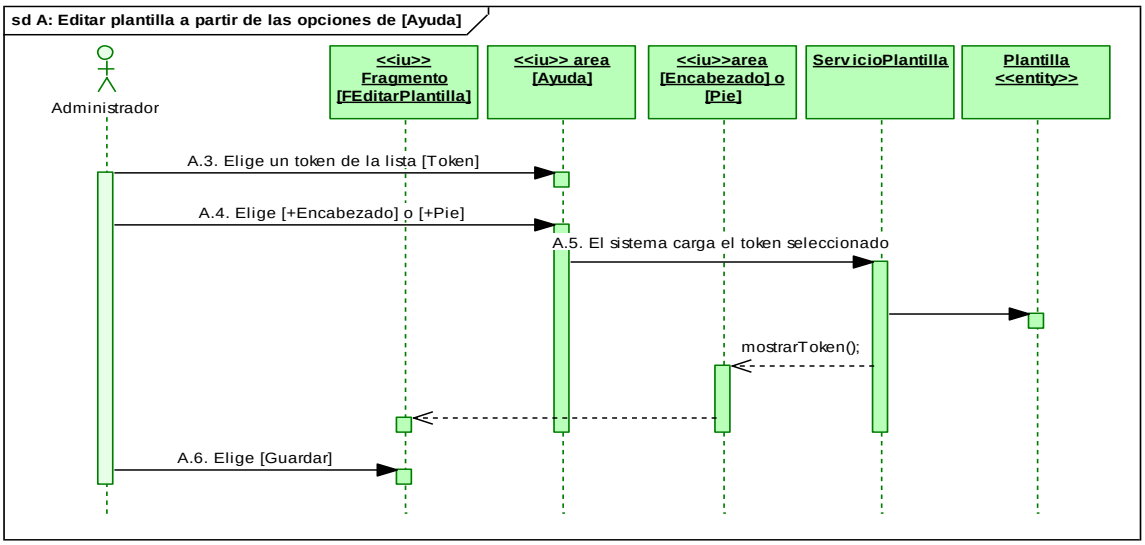


Fig.121. DS Curso Alterno: Editar plantilla a partir de las opciones de [Ayuda]

B. Campos requeridos

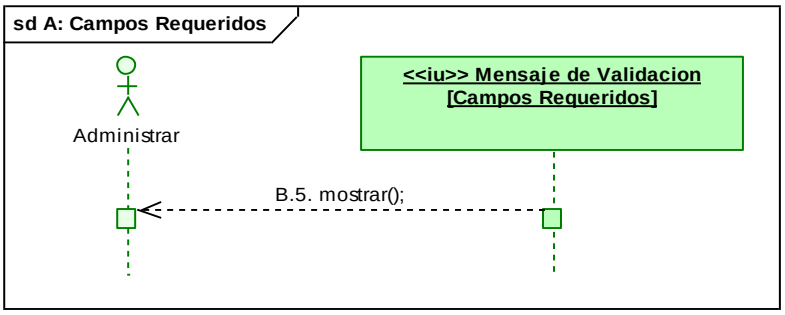


Fig.122. DS Curso Alterno: Campos Requeridos

C. Nombre de plantilla duplicado

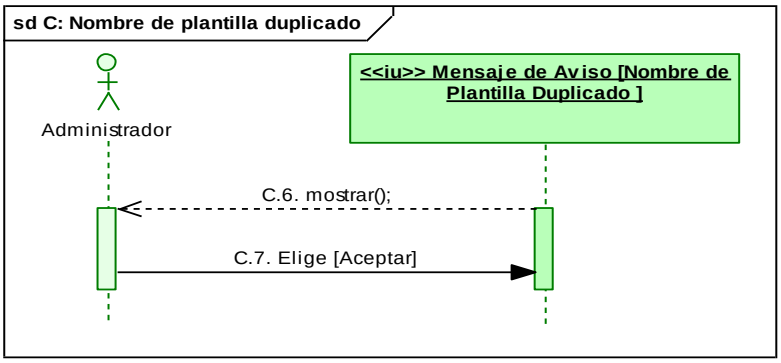


Fig.123. DS Curso Alterno: Nombre de plantilla duplicado

MT16: Eliminar Plantilla

Curso Normal de Eventos

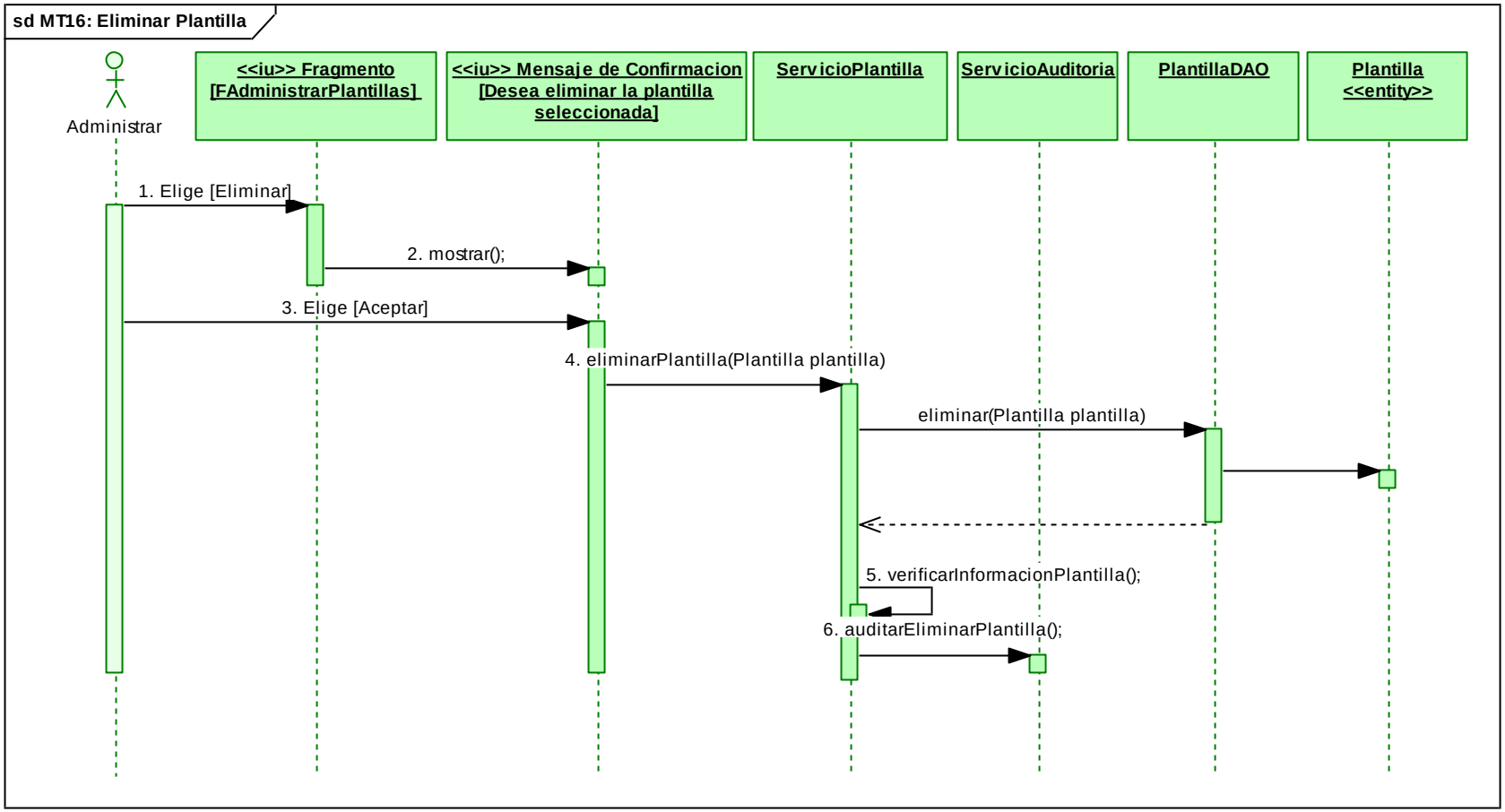


Fig.124. DS Curso Normal: Eliminar Plantilla

CASO DE USO CU06: ADMINISTRAR DEPARTAMENTOS

MT17: Crear Departamento

Curso Normal de Eventos

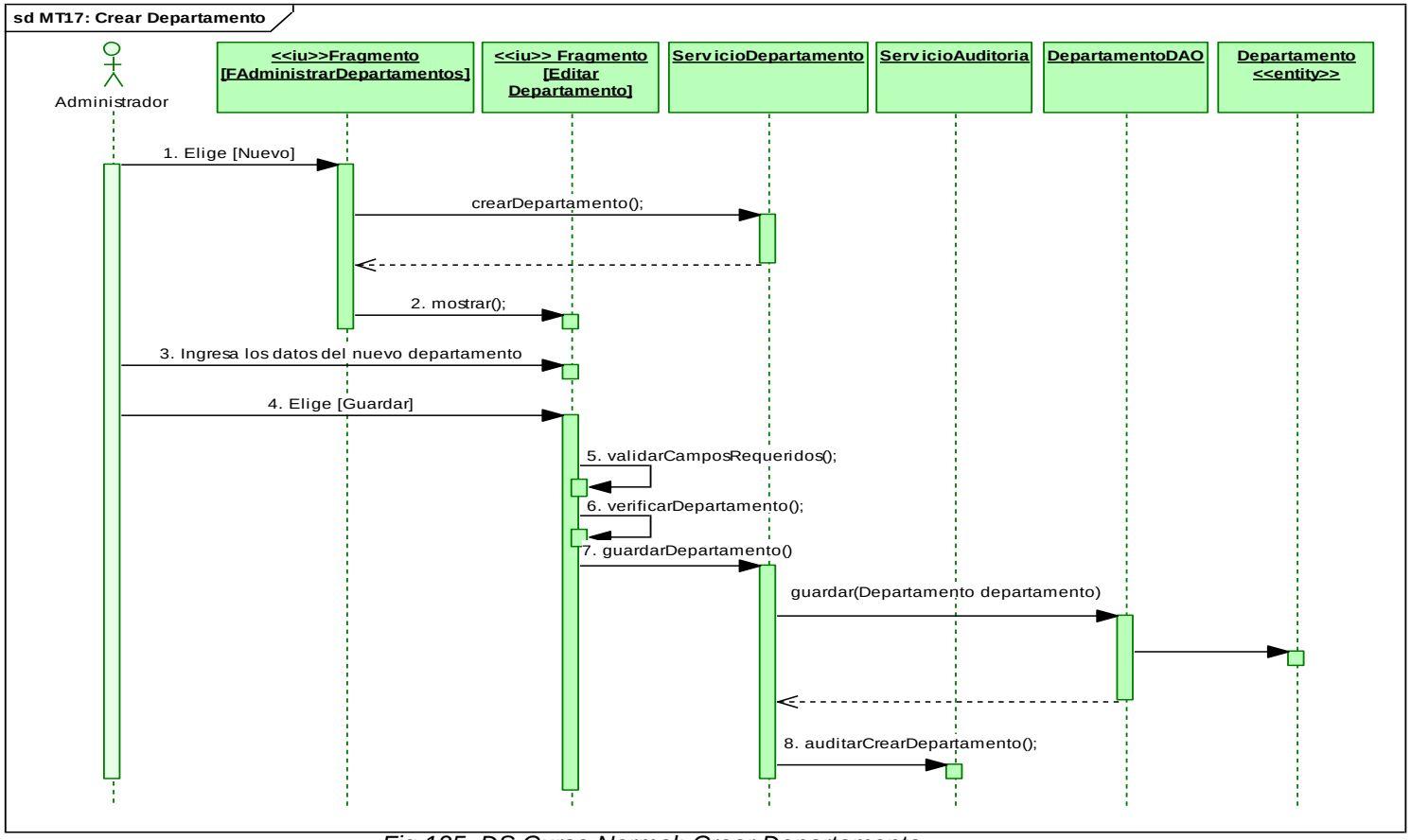


Fig.125. DS Curso Normal: Crear Departamento

Cursos Alternos de Eventos

A. Campos Requeridos

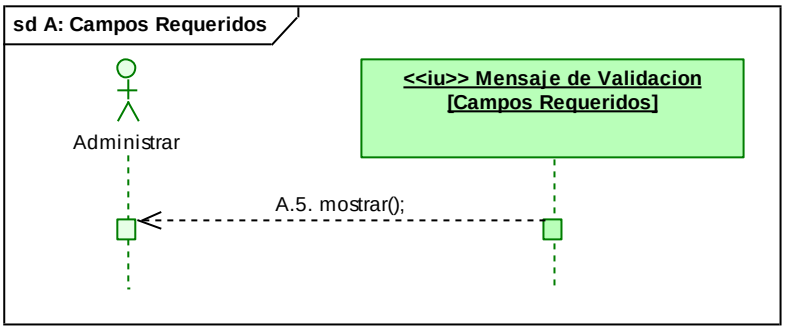


Fig.126. DS Curso Alterno: Campos Requeridos

B. Nombre de departamento duplicado

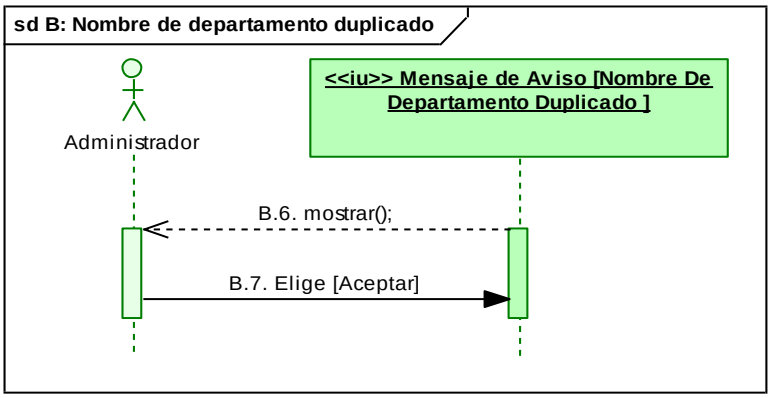


Fig.127. DS Curso Alterno: Nombre de departamento duplicado

MT18: Editar Departamento

Curso Normal de Eventos

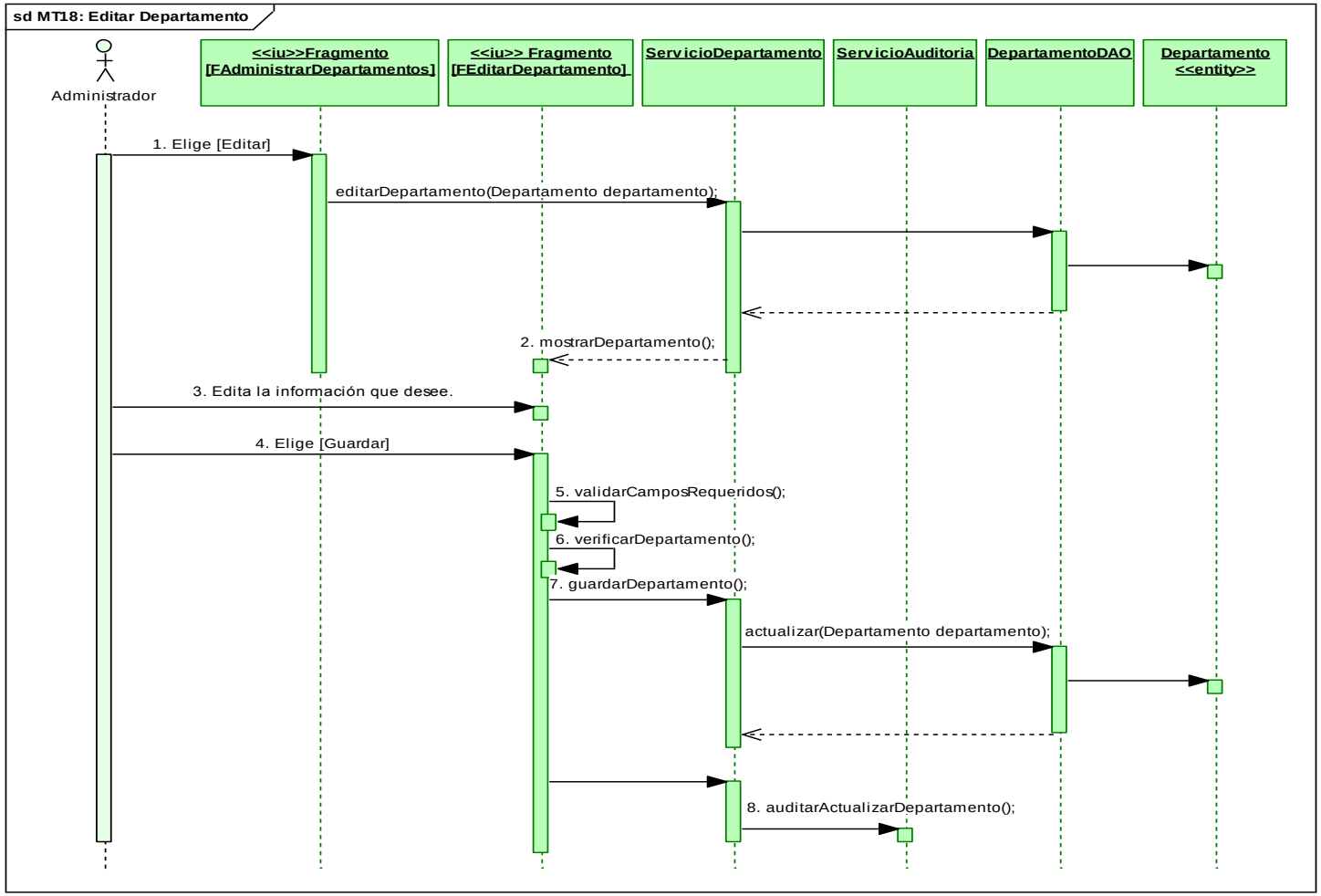


Fig.128. DS Curso Normal: Editar Departamento

Cursos Alternos de Eventos

A. Campos Requeridos

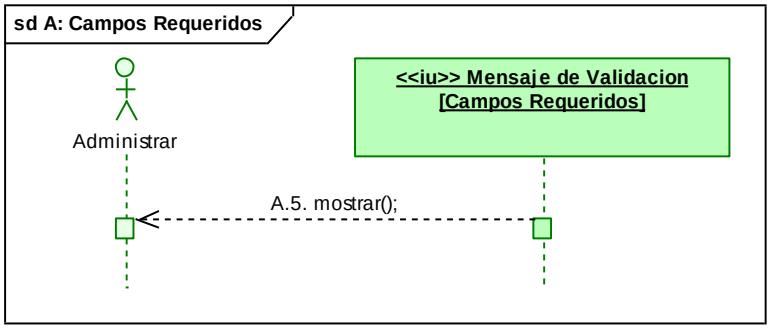


Fig.129. DS Curso Alterno: Campos Requeridos

B. Nombre de departamento duplicado

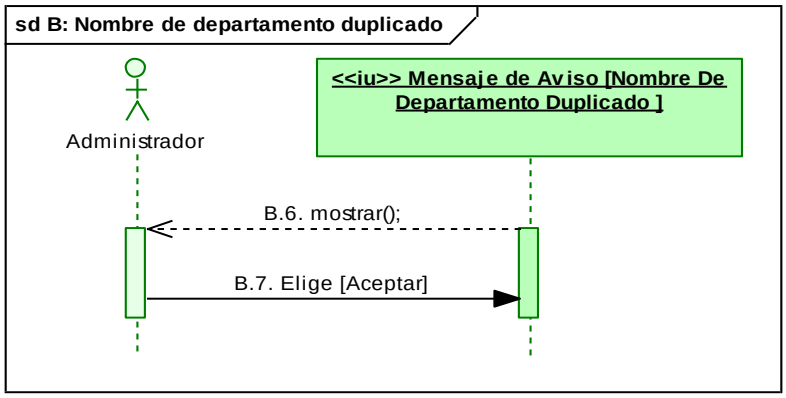


Fig.130. DS Curso Alterno: Nombre de departamento duplicado

MT19: Eliminar Departamento

Curso Normal de Eventos

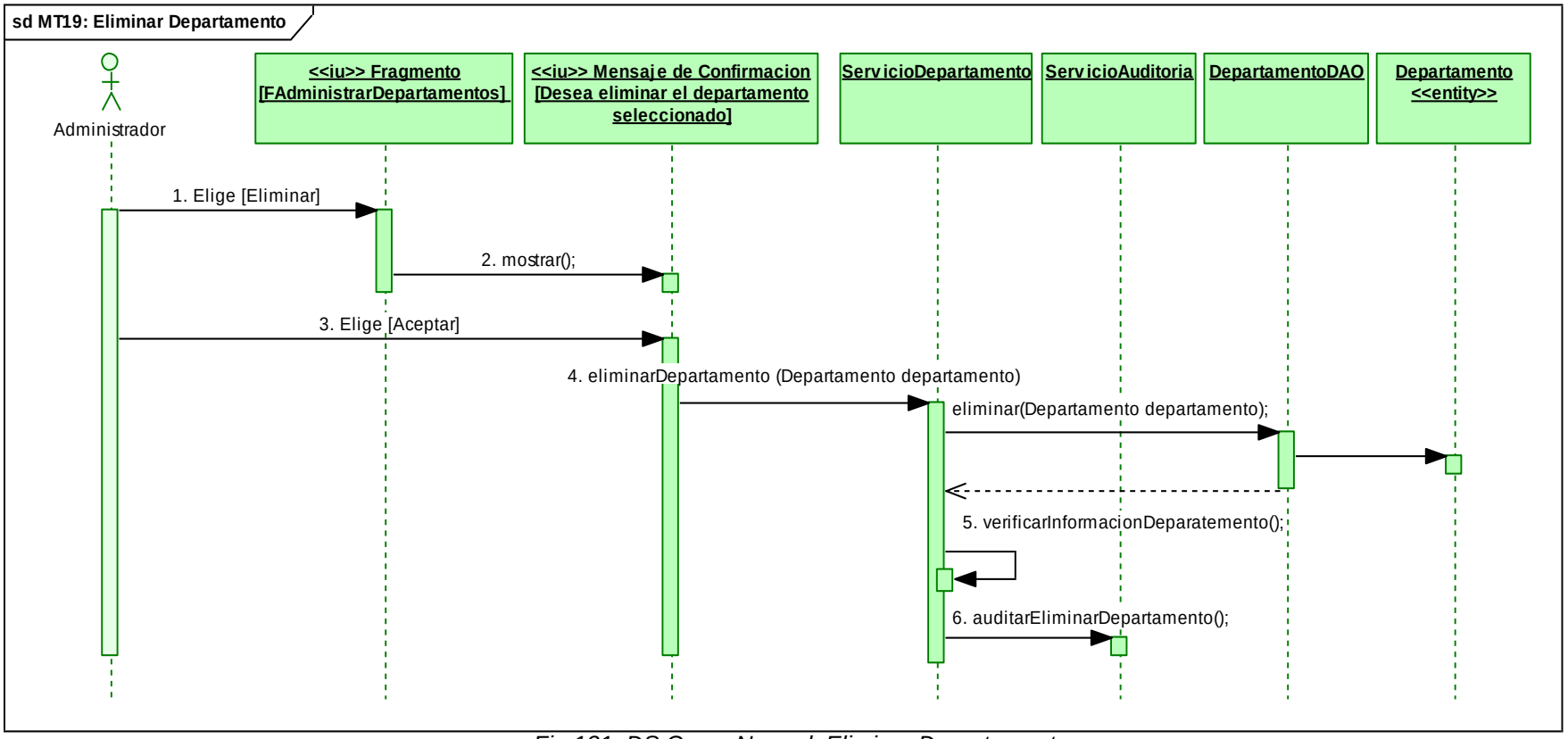


Fig.131. DS Curso Normal: Eliminar Departamento

CASO DE USO CU07: ADMINISTRAR PARÁMETROS

MT20: Editar Parámetros

Curso Normal de Eventos

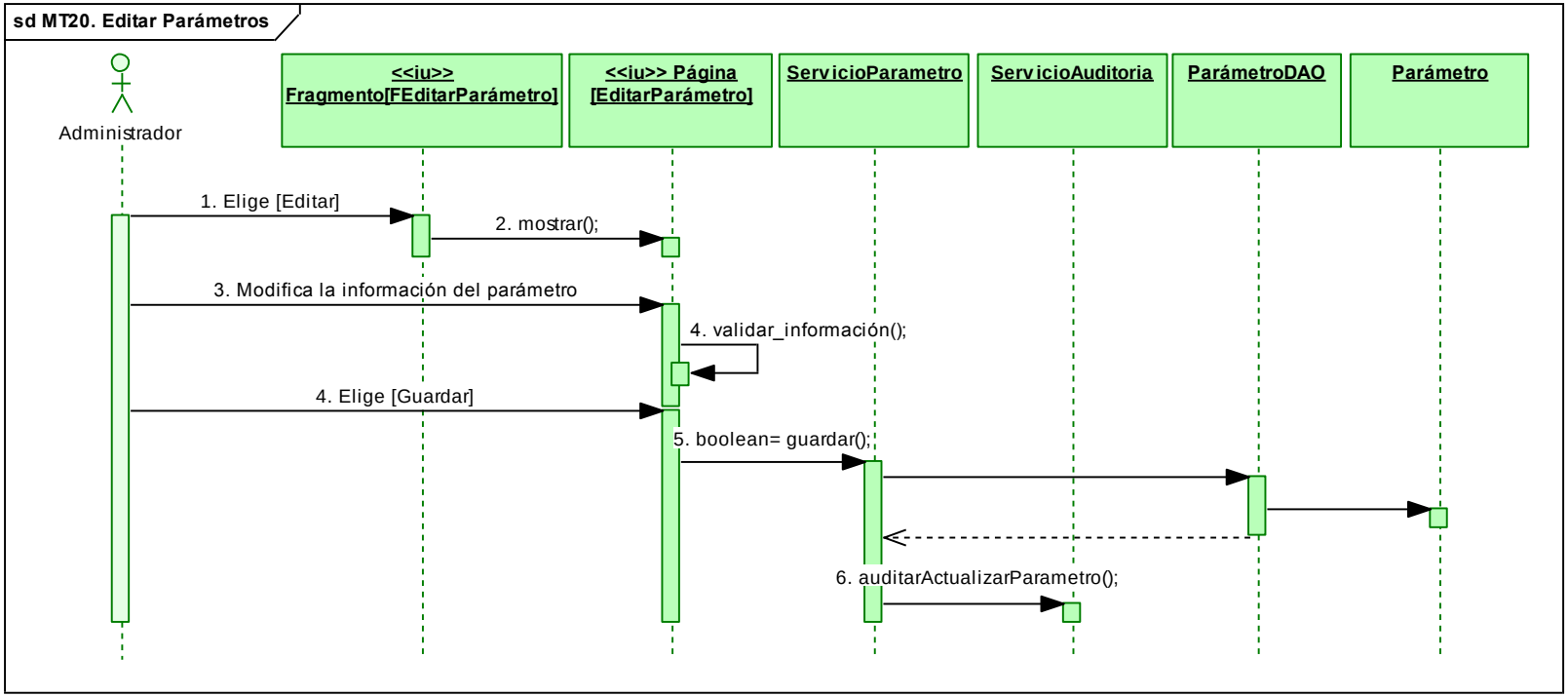


Fig.132. DS Curso Normal: Editar Parámetros

CASO DE USO CU08: GESTIONAR DOCUMENTOS ELECTRÓNICOS

MT21: Crear/Enviar Documentos

Curso Normal de Eventos

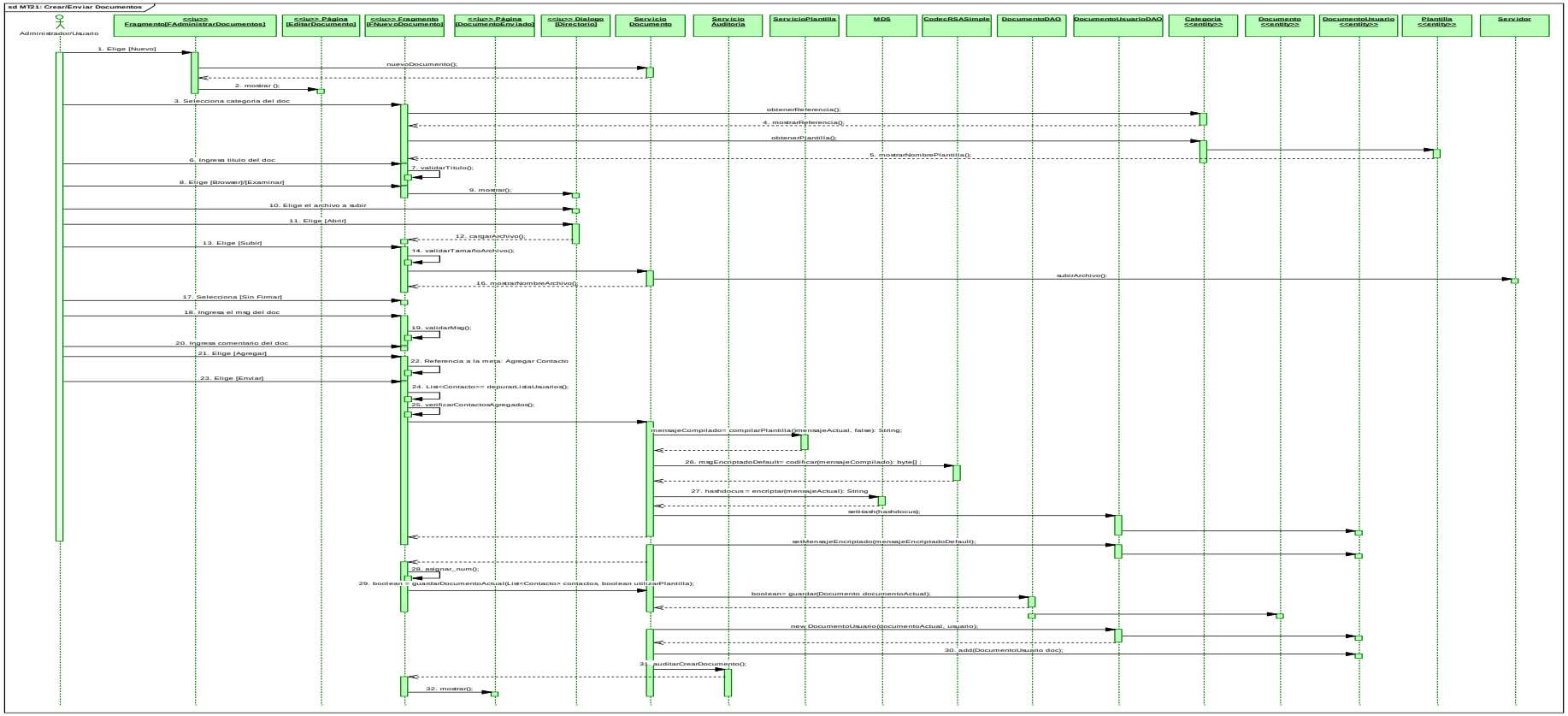


Fig.133. DS Curso Normal. Crear/Enviar Documentos

Cursos Alternos de Eventos

A. Campos Requeridos

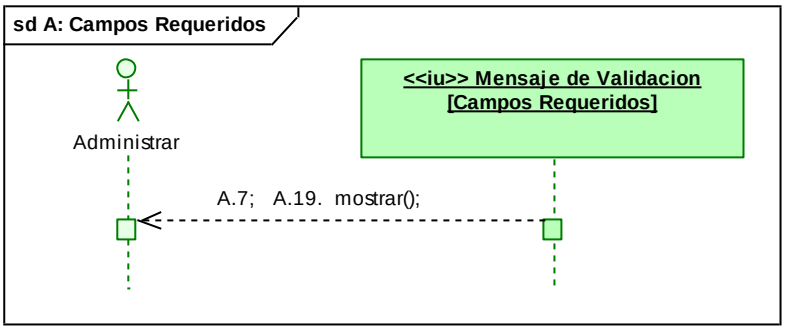


Fig.134. DS Curso Alterno: Campos Requeridos

B. Tamaño del archivo excede el rango permitido

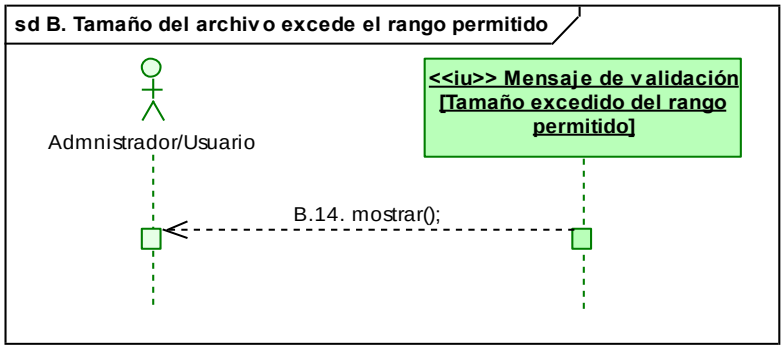


Fig.135. DS Curso Alterno: Tamaño del archivo excede el rango permitido

C. Eliminar archivo adjunto

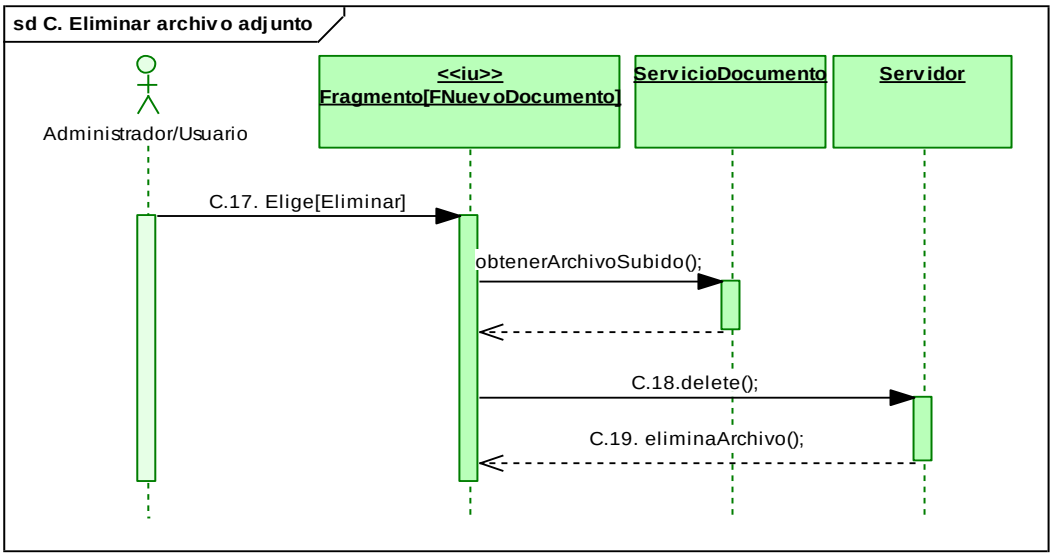


Fig.136. DS Curso Alterno: Eliminar archivo adjunto

D. Firmar documento

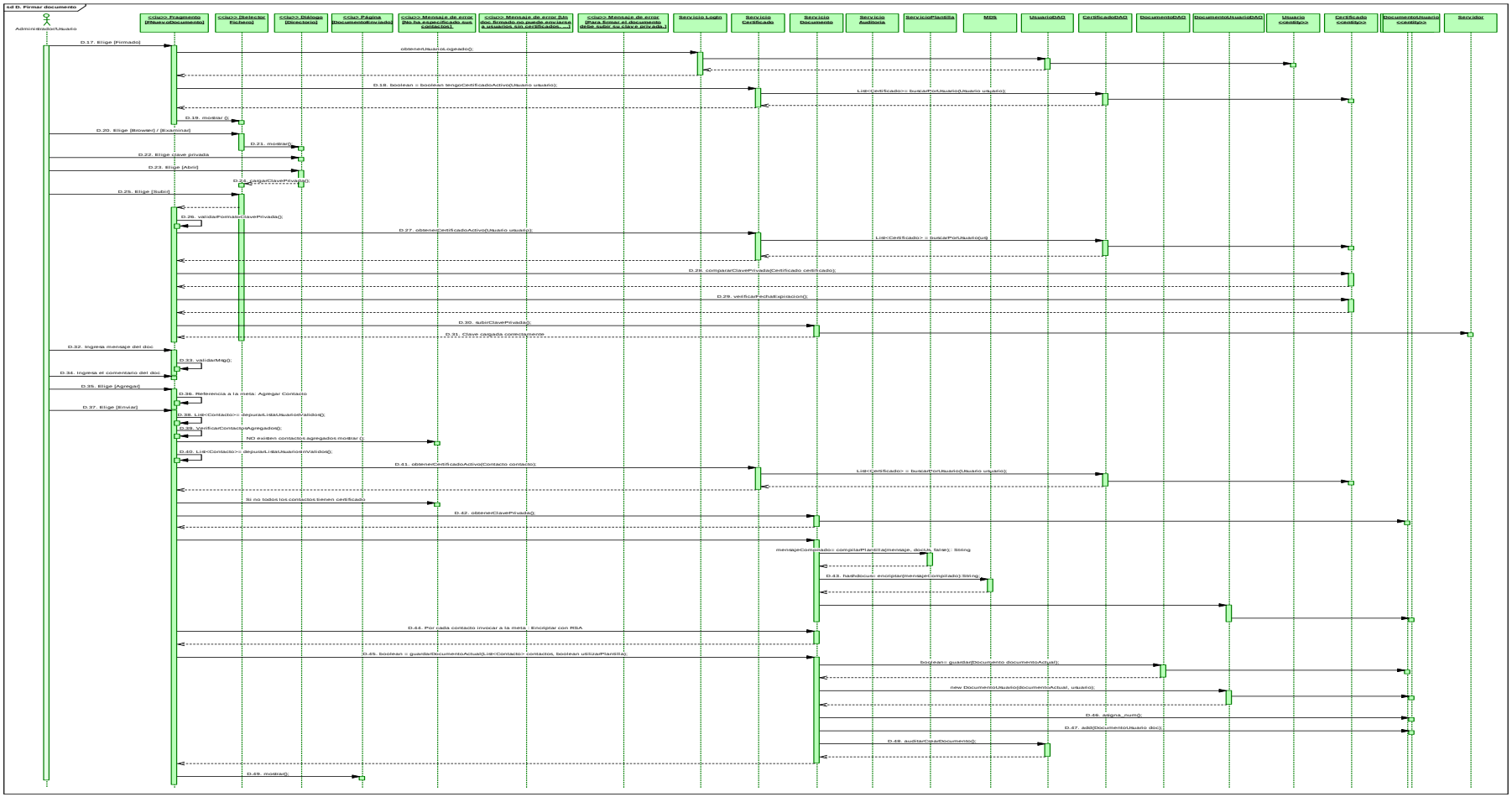


Fig.137. DS Curso Alterno: Firmar documento

E. Vista Previa

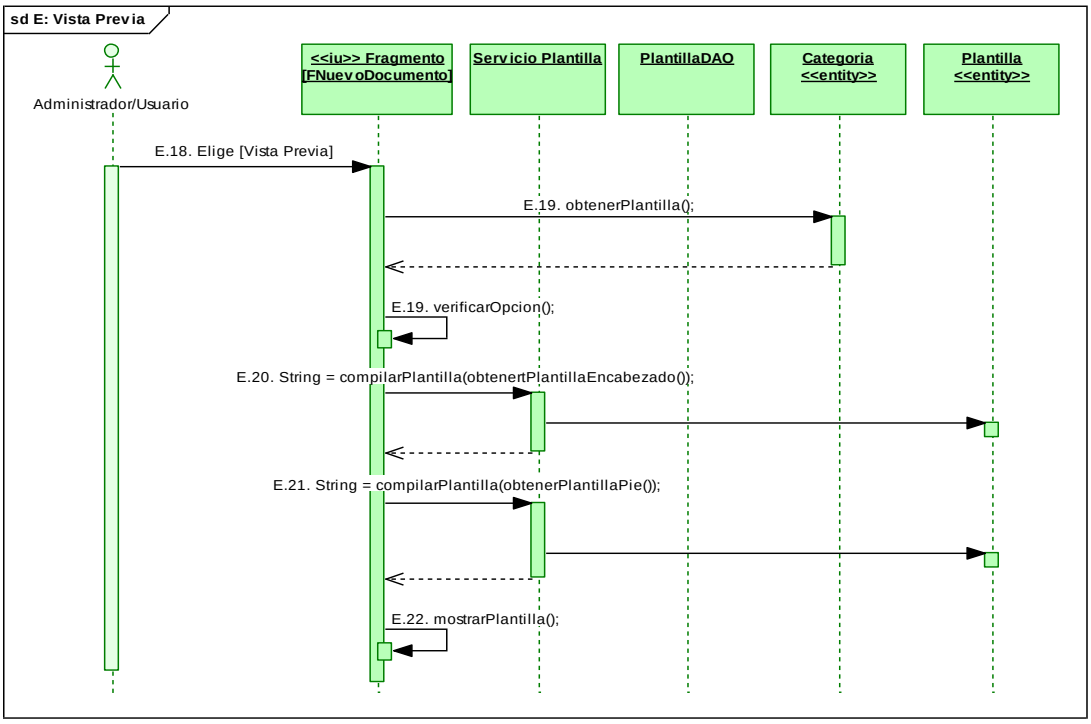


Fig.138. DS Curso Alterno: Vista Previa

F. No existen contactos especificados

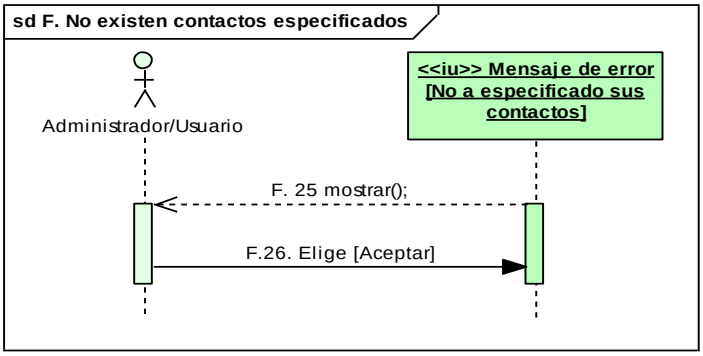


Fig.139. DS Curso Alterno: No existen contactos especificados

G. Ver Bandeja Entrada/Salida

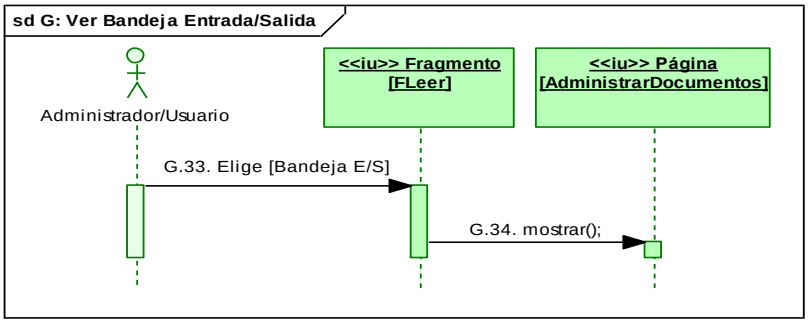


Fig.140. DS Curso Alterno: Ver Bandeja Entrada/Salida

H. Crear documento una vez que se envió uno nuevo

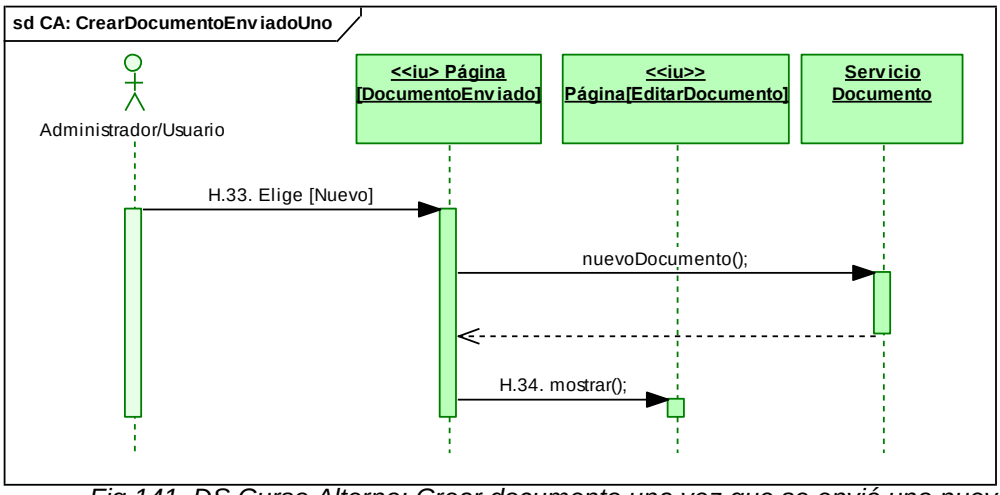


Fig.141. DS Curso Alterno: Crear documento una vez que se envió uno nuevo

MT22: Encriptar con RSA

Curso Normal de Eventos

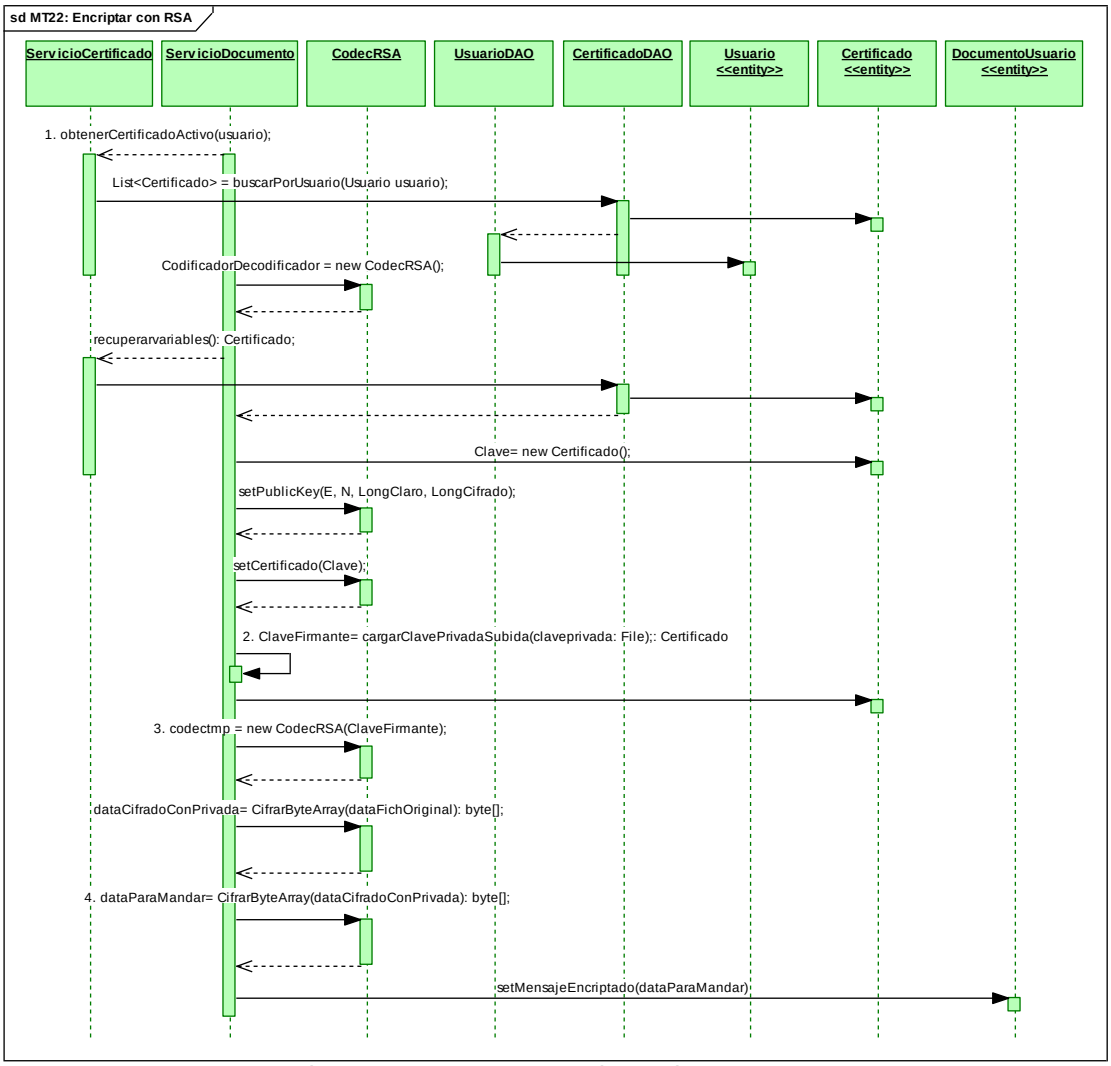


Fig.142. DS Curso Normal: Encriptar con RSA

MT23: Buscar Contacto

Curso Normal de Eventos

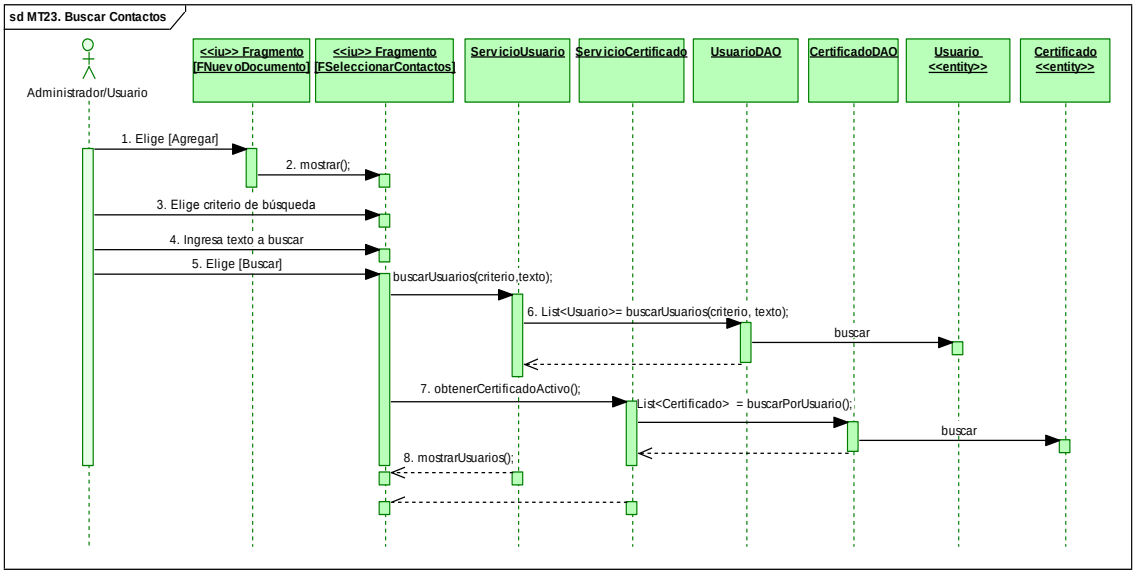


Fig.143. DS Curso Normal: Buscar Contacto

MT24: Agregar Contacto

Curso Normal de Eventos

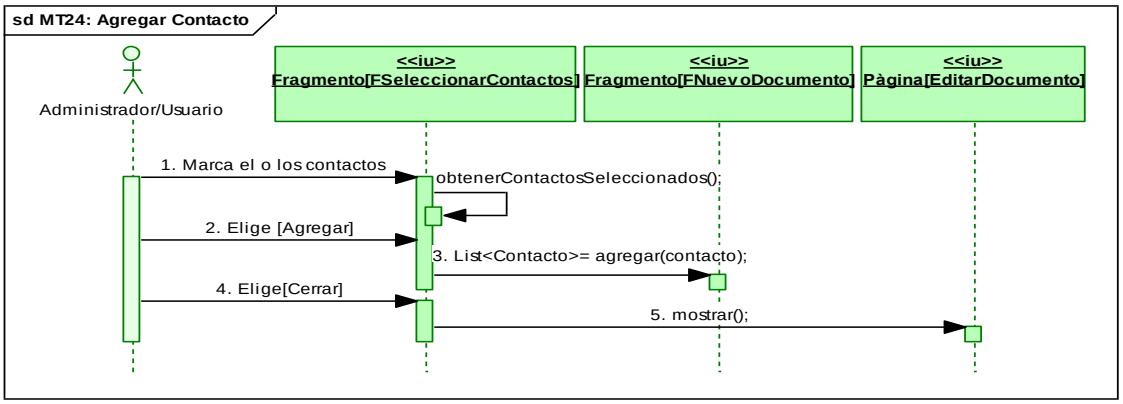


Fig. 144. DS Curso Normal: Agregar Contacto

Cursos Alternos de Eventos

A. Marcar Todos

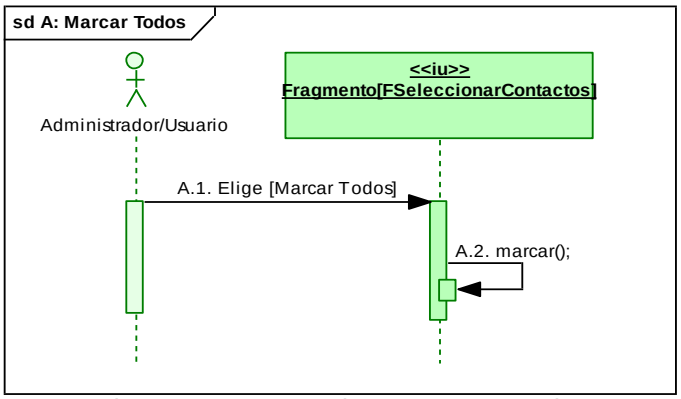


Fig.145. DS Curso Alterno: Marcar Todos

B. Desmarcar Todos

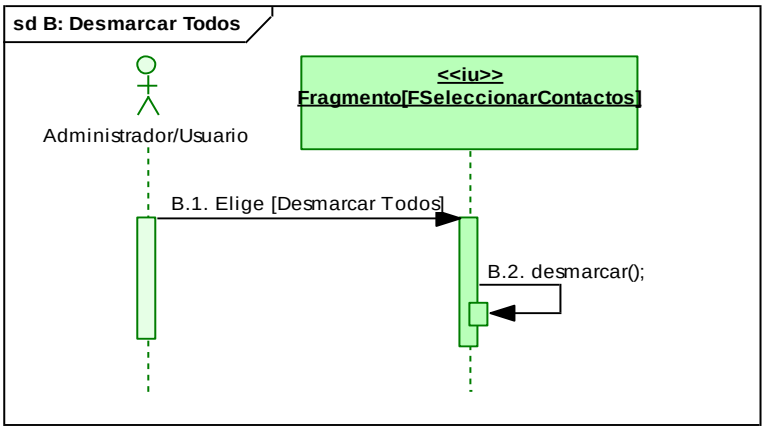


Fig.146. DS Curso Alterno: Desmarcar Todos

C. Cerrar

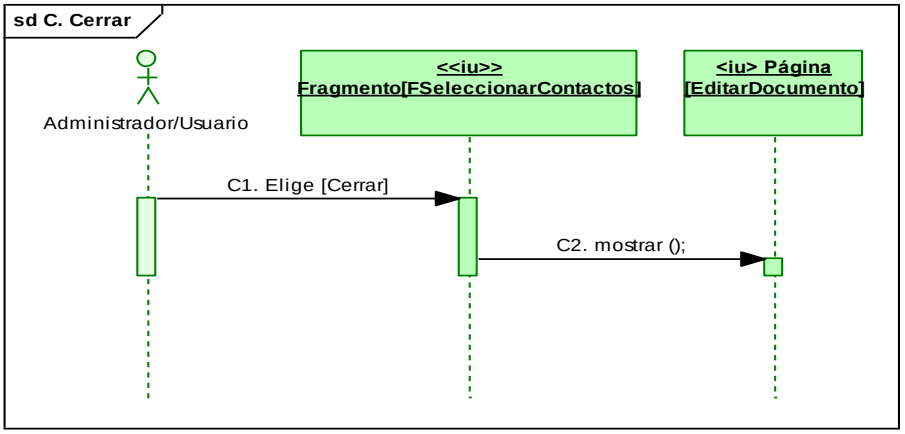


Fig.147. DS Curso Alterno: Cerrar

MT25: Eliminar Contacto

Curso Normal de Eventos

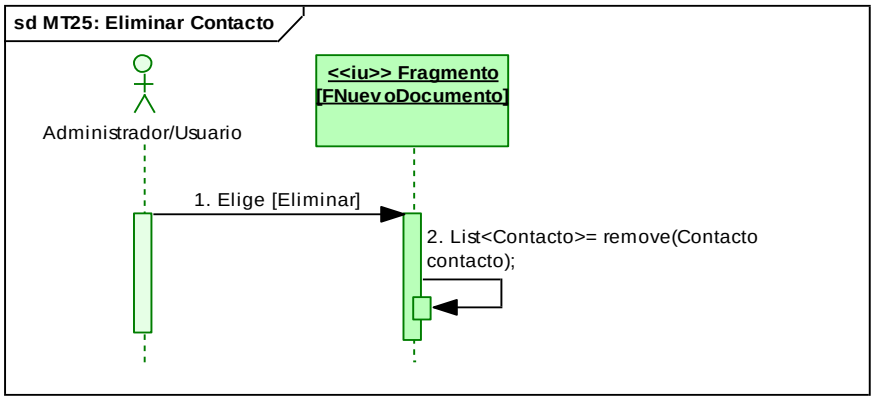


Fig.148. DS Curso Normal: Eliminar Contacto

Cursos Alternos de Eventos

A. Limpiar Lista

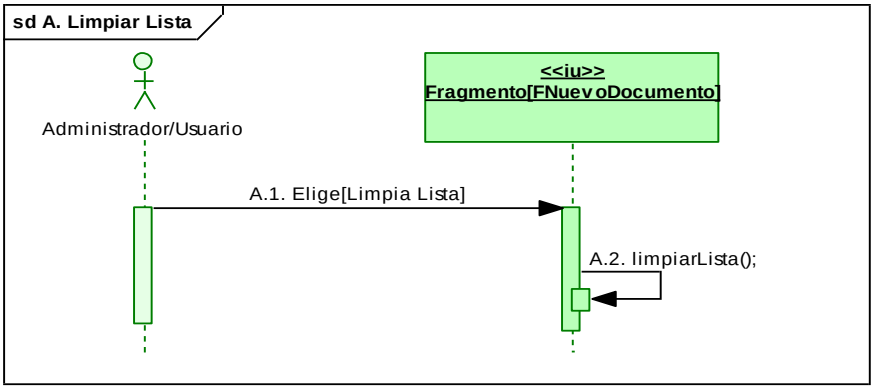


Fig.149. DS Curso Alterno: Limpiar Lista

B. Depurar Lista

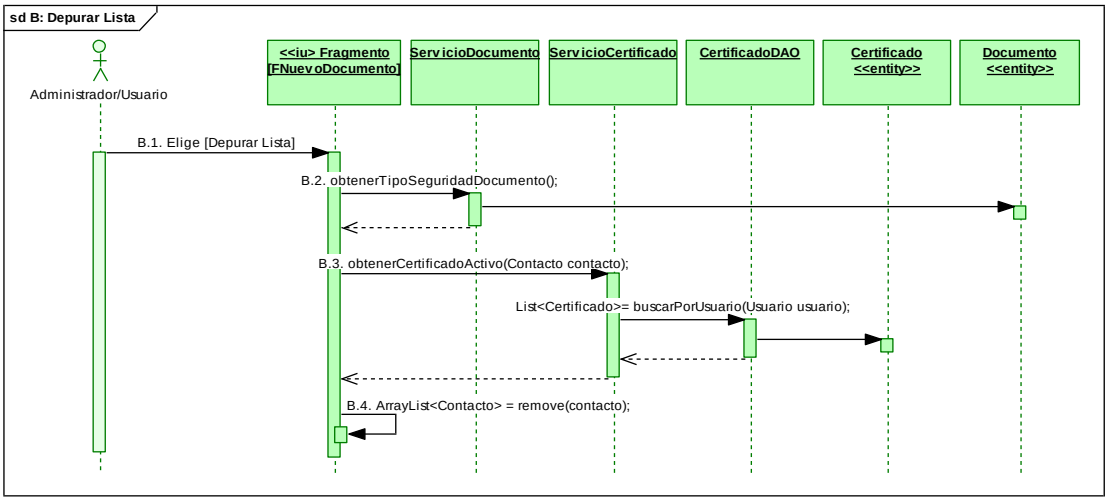


Fig.150. DS Curso Alterno: Depurar Lista

MT26: Leer Documentos Recibidos

Curso Normal de Eventos

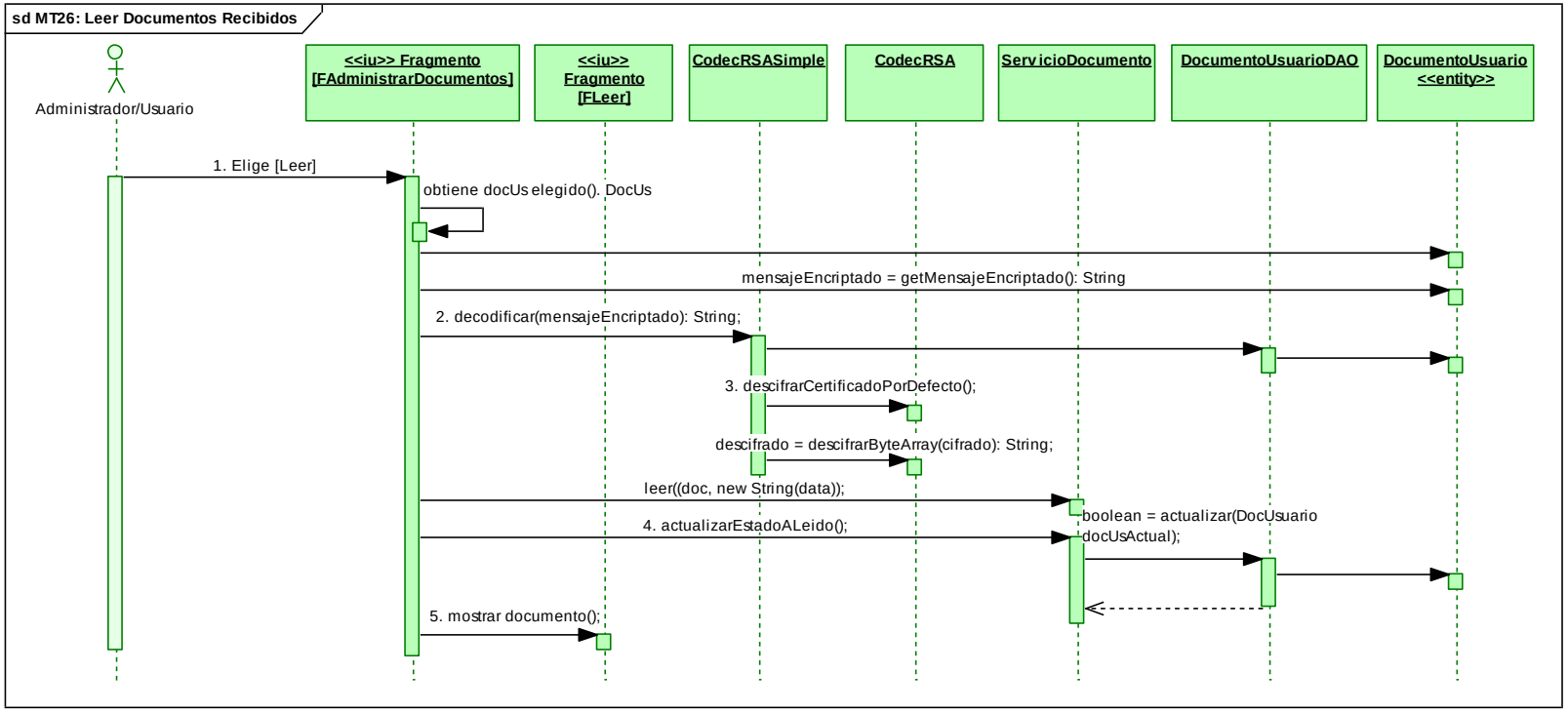


Fig.151. DS Curso Normal: Leer Documentos Recibidos

Cursos Alternos de Eventos

A. Leer Documento Firmado

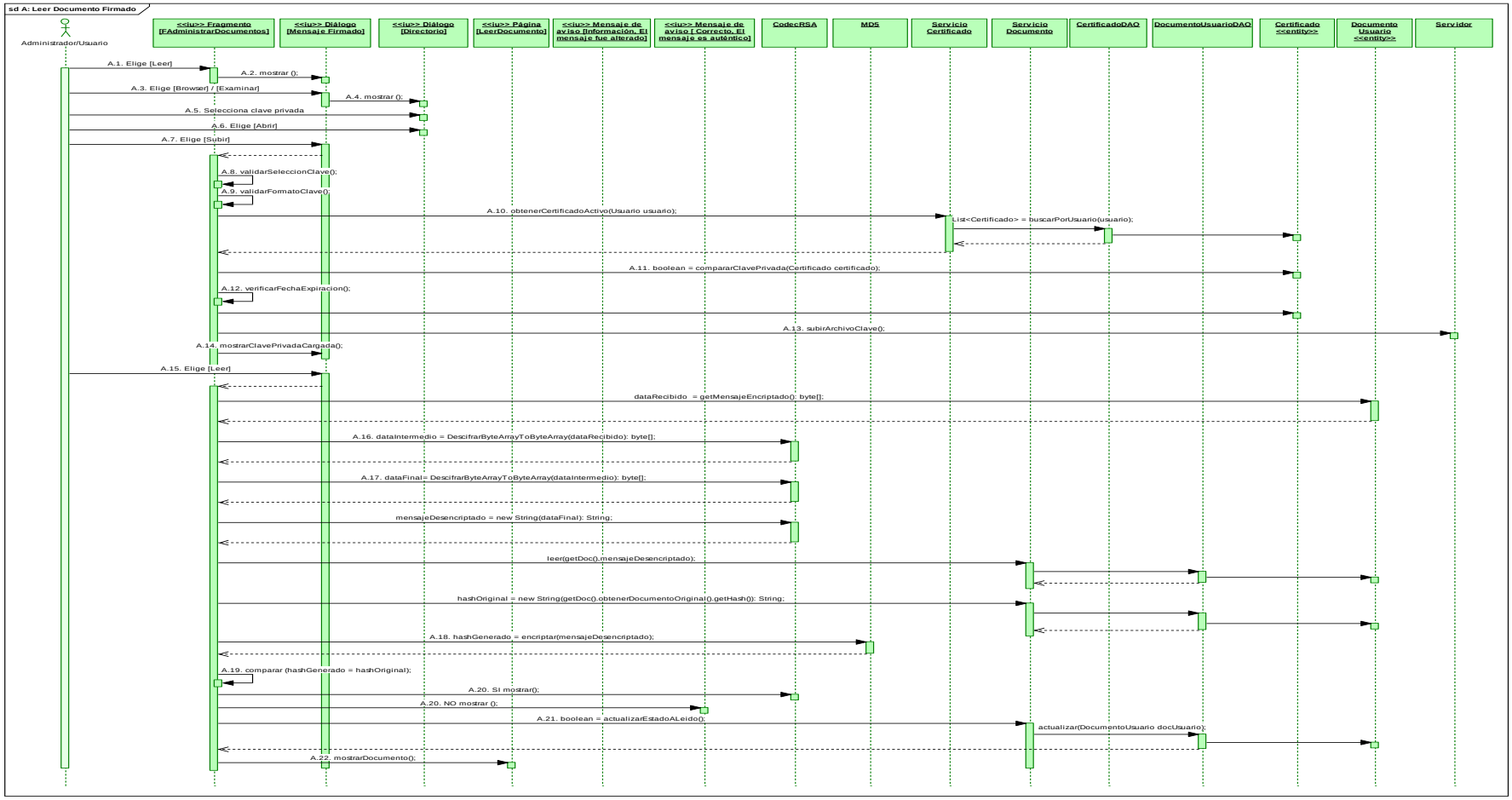


Fig.152. DS Curso Alterno: Leer Documento Firmado

B. Descargar archivo adjunto

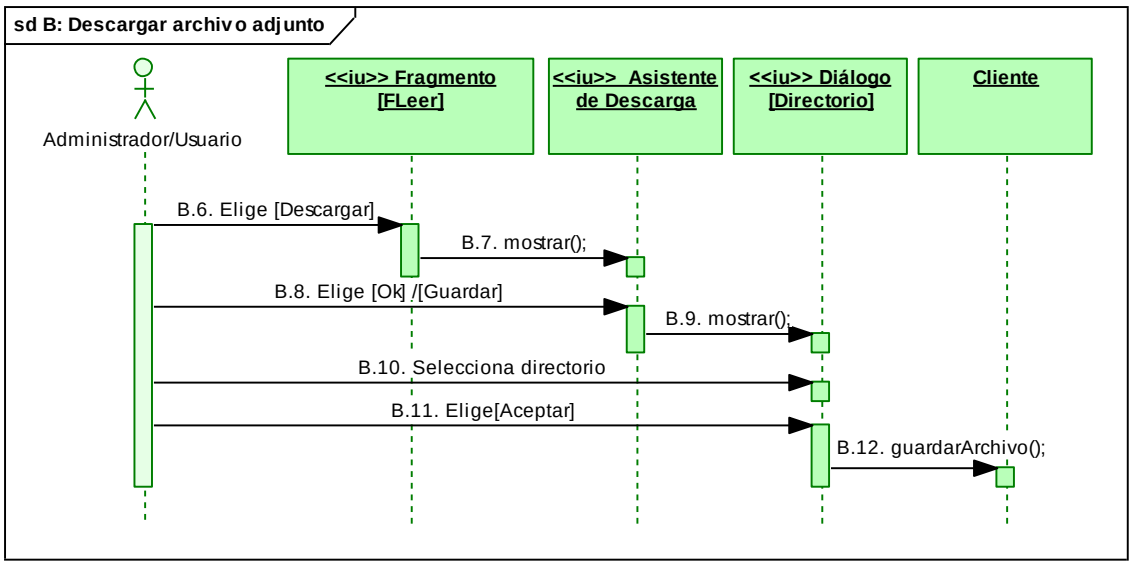


Fig.153. DS Curso Alterno: Descargar archivo adjunto

C. Ver Bandeja Entrada/Salida

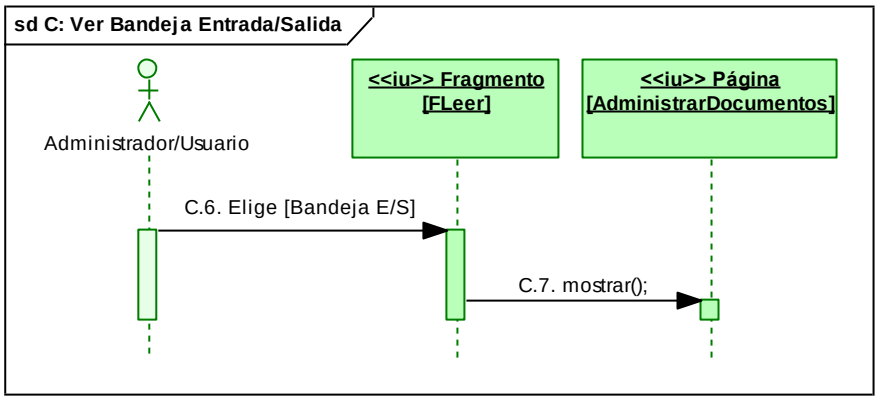


Fig.154. DS Curso Alterno: Ver Bandeja Entrada/Salida

D. Reenviar

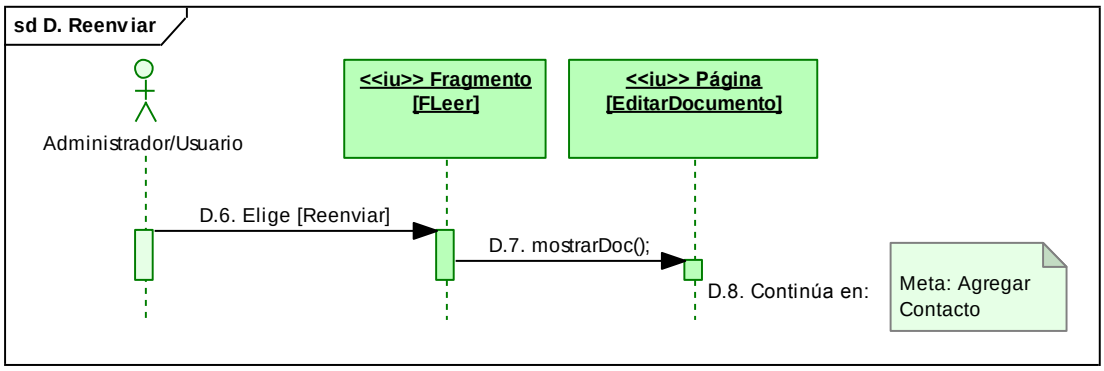


Fig.155. DS Curso Alterno: Reenviar

MT27: Eliminar Bandeja de Entrada.

Curso Normal de Eventos

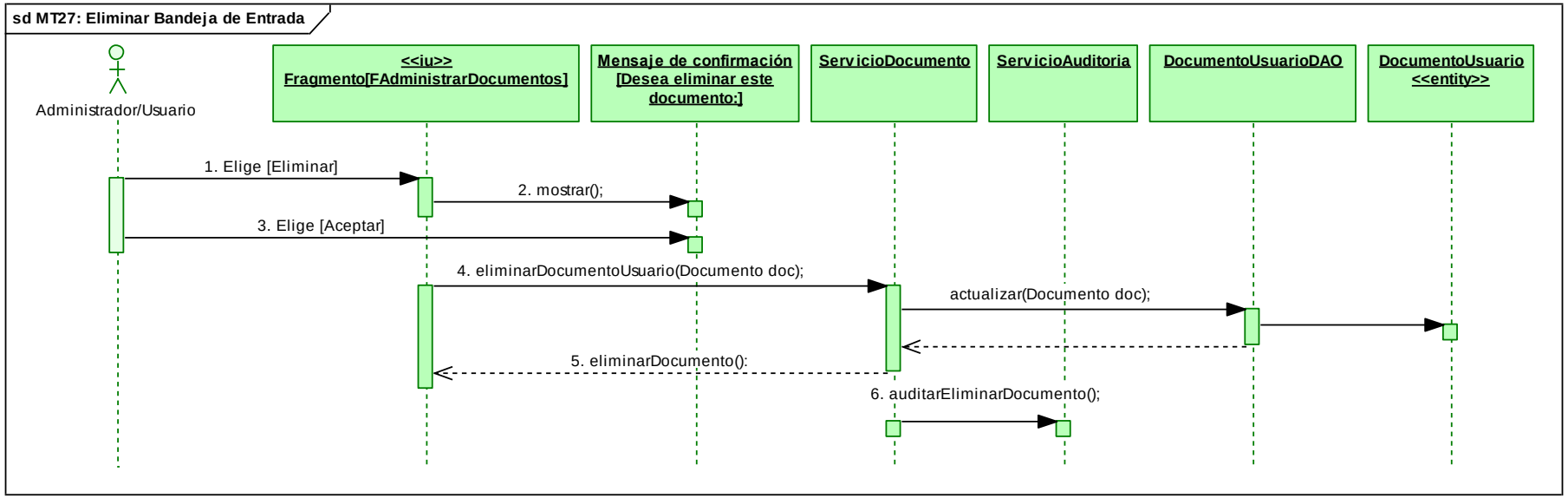


Fig.156. DS Curso Normal: Eliminar Bandeja de Entrada

MT28: Crear un Borrador

Curso Normal de Eventos

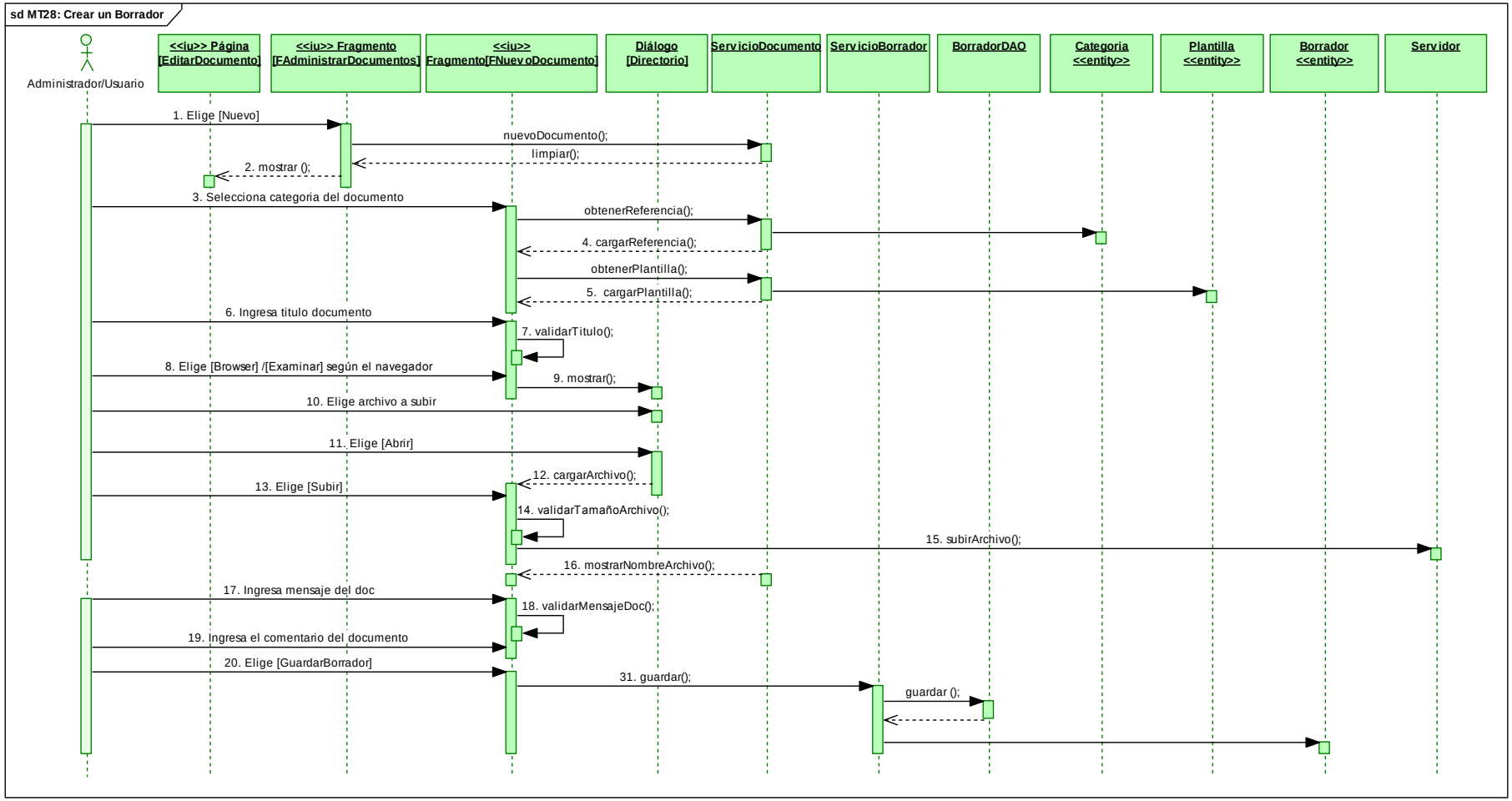


Fig.157. DS Curso Normal: Crear un Borrador

Cursos Alternos de Eventos

A. Campos Requeridos

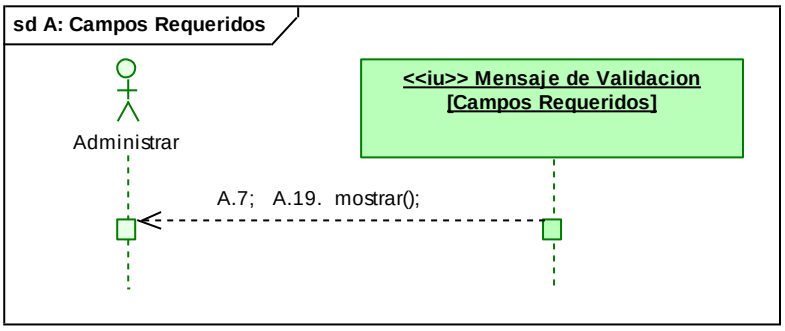


Fig.158. DS Curso Alterno: Campos Requeridos

B. Tamaño del archivo excede el rango permitido

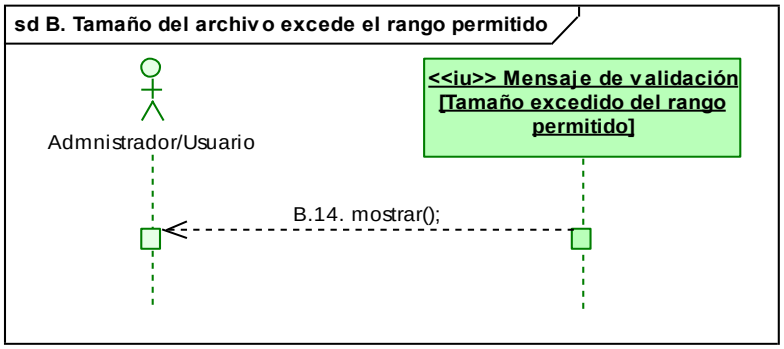


Fig.159. DS Curso Alterno: Tamaño del archivo excede el rango permitido

C. Eliminar archivo adjunto

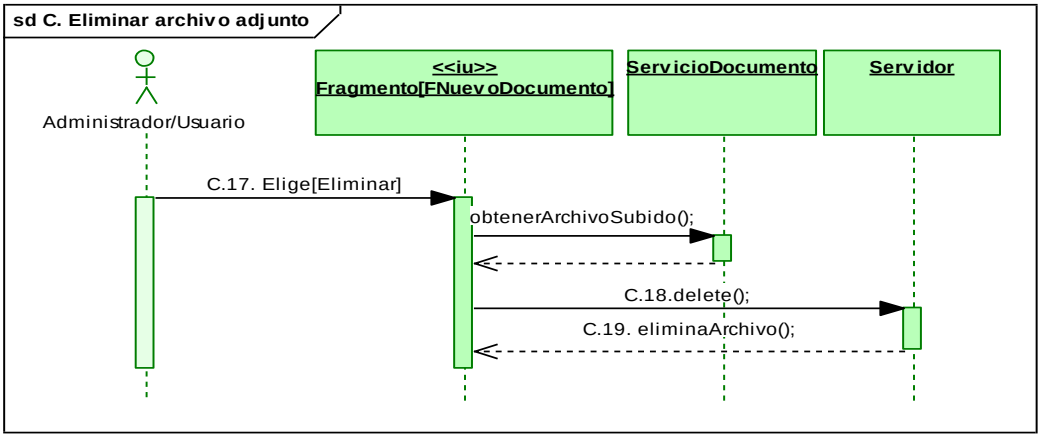


Fig.160. DS Curso Alterno: Eliminar archivo adjunto

MT29: Editar un Borrador

Curso Normal de Eventos

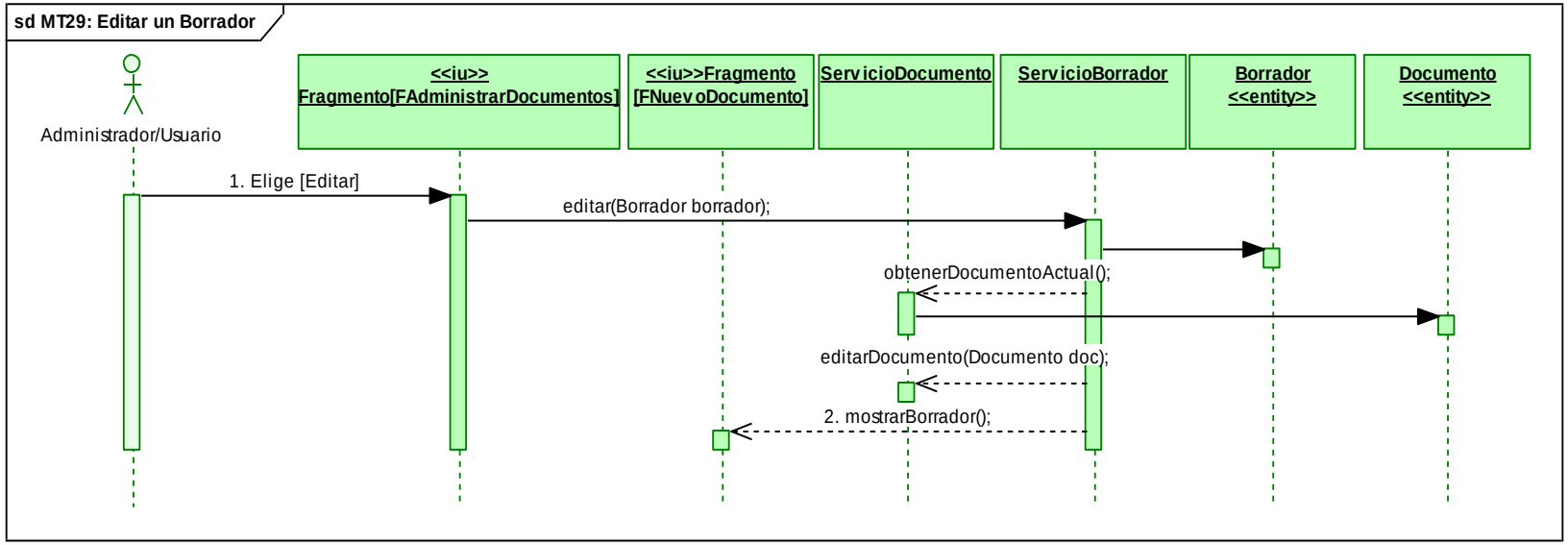


Fig.161. DS Curso Normal: Editar un Borrador

MT30: Eliminar un Borrador

Curso Normal de Eventos

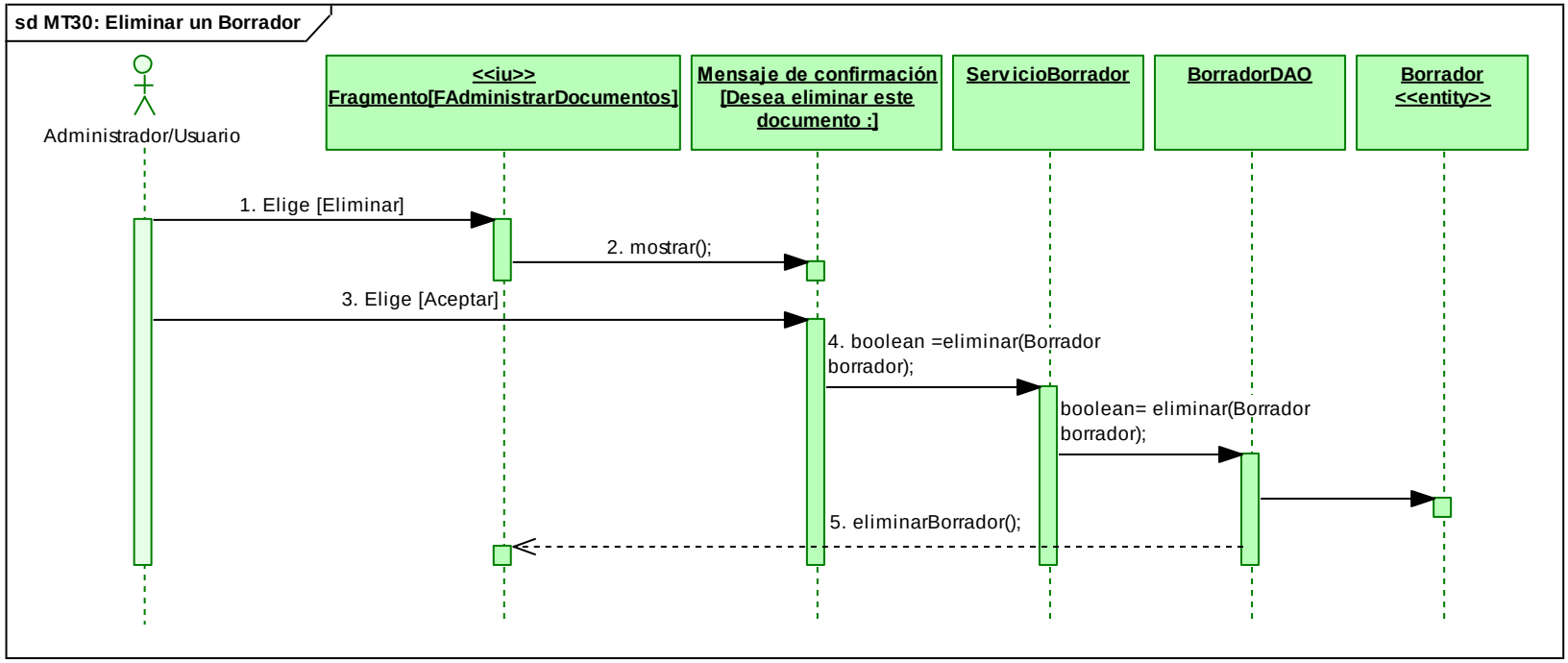


Fig.162. DS Curso Normal: Eliminar un Borrador

MT31: Presentar Documentos

Curso Normal de Eventos

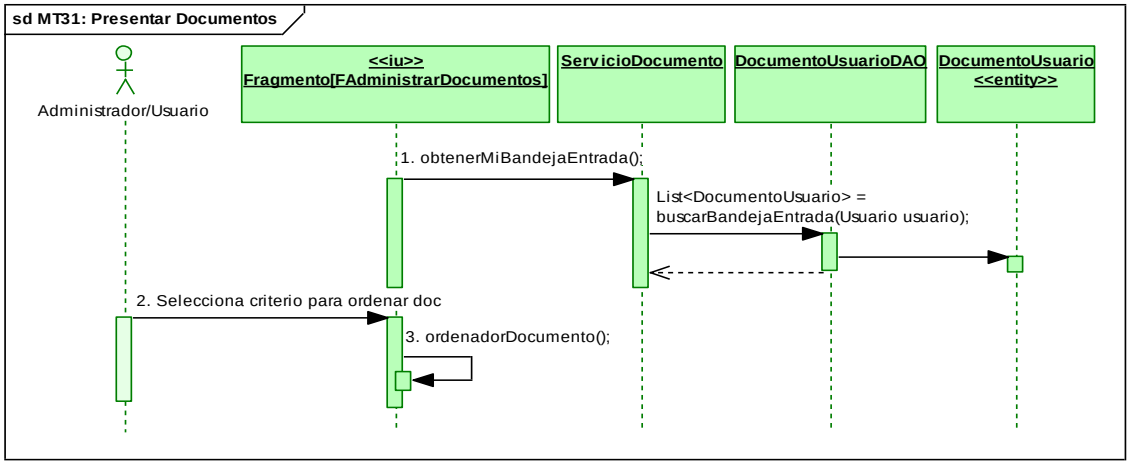


Fig.163. DS Curso Normal: Presentar Documentos

Cursos Alternos de Eventos

A. Presentar bandeja de salida

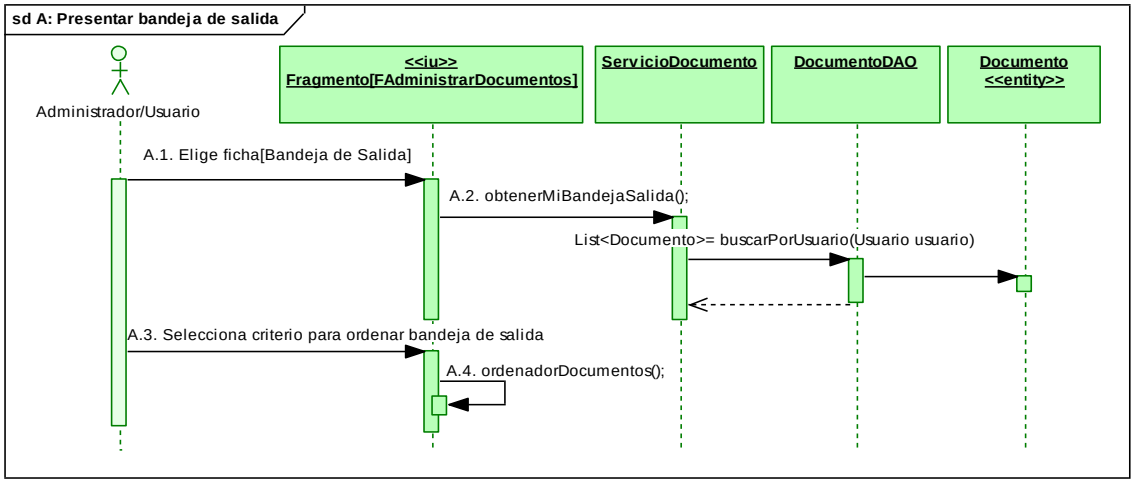


Fig.164. DS Curso Alterno: Presentar bandeja de salida

B. Presentar documentos eliminados

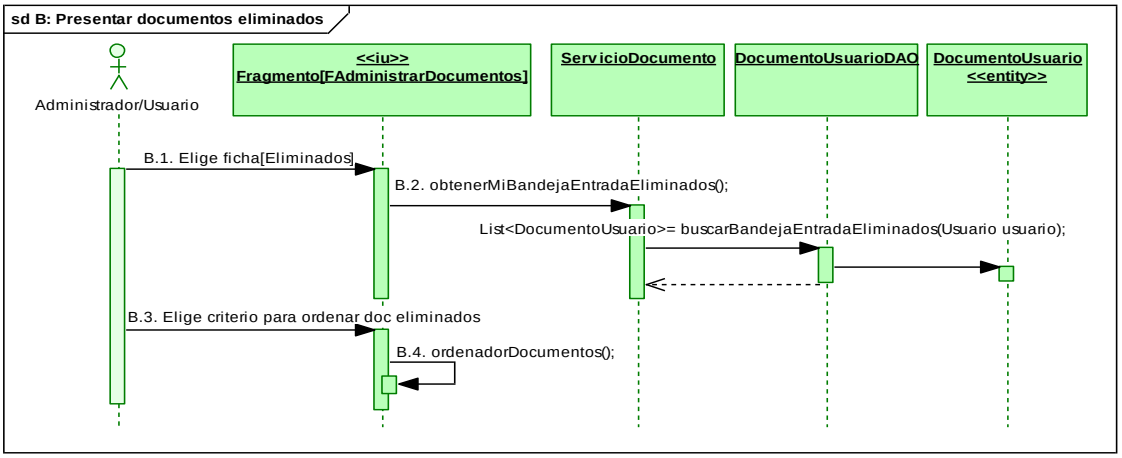


Fig.165. DS Curso Alterno: Presentar documentos eliminados

C. Presentar borradores

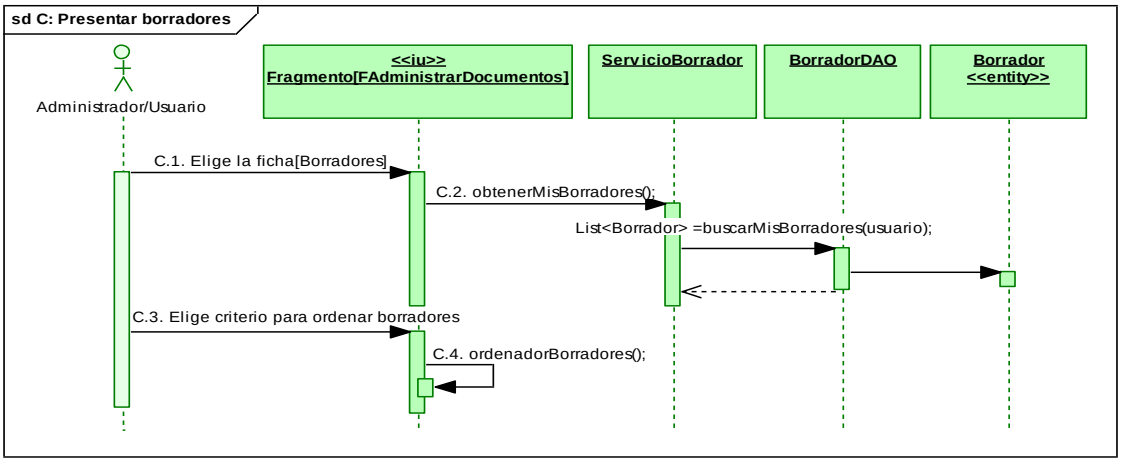


Fig.166. DS Curso Alterno: Presentar borradores

MT32: Buscar Documentos

Curso Normal de Eventos

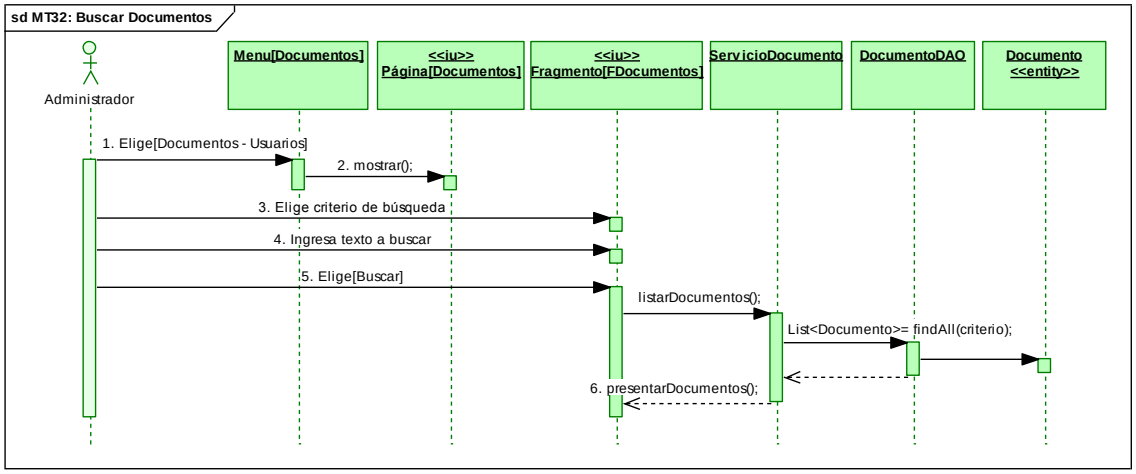


Fig.167. DS Curso Normal: Buscar Documentos

CASO DE USO CU09: GENERAR REPORTES

MT33: Generar Reportes

Curso Normal de Eventos

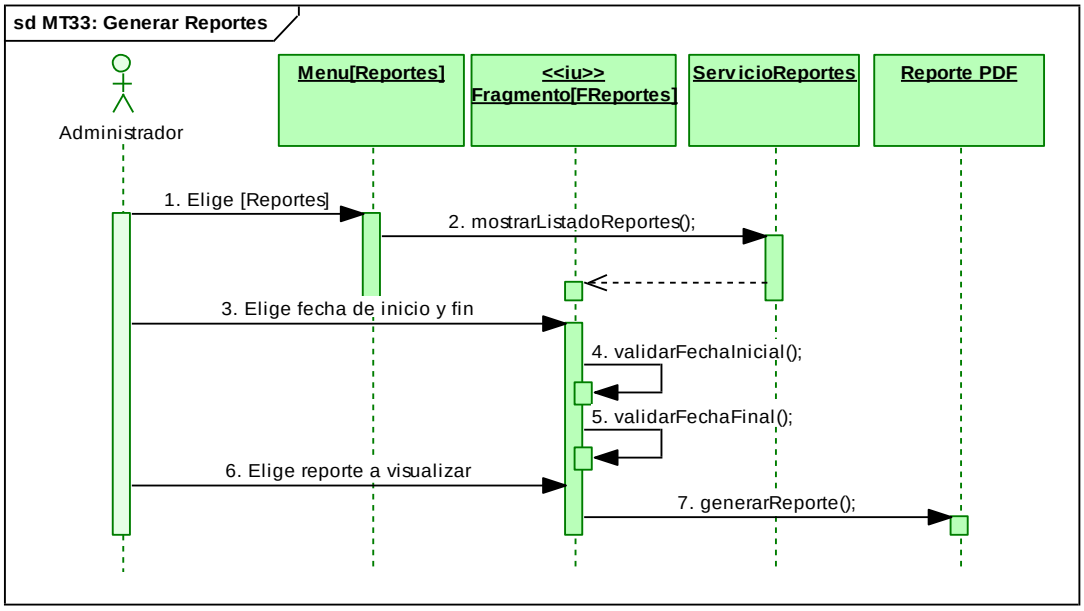


Fig.168. DS Curso Normal: Generar Reportes

Cursos Alternos de Eventos

A. Fecha Inicial mayor a la final

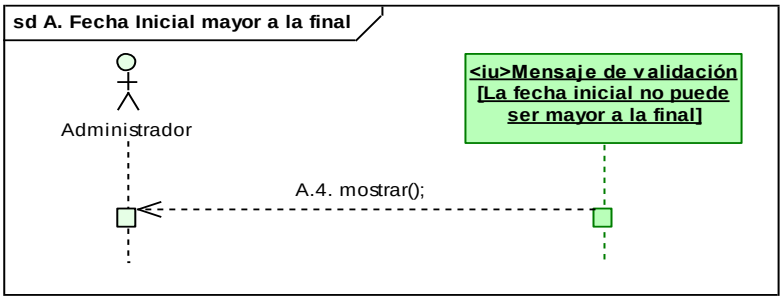


Fig.169. DS Curso Alterno: Fecha Inicial mayor a la final

B. Fecha final menor a la inicial

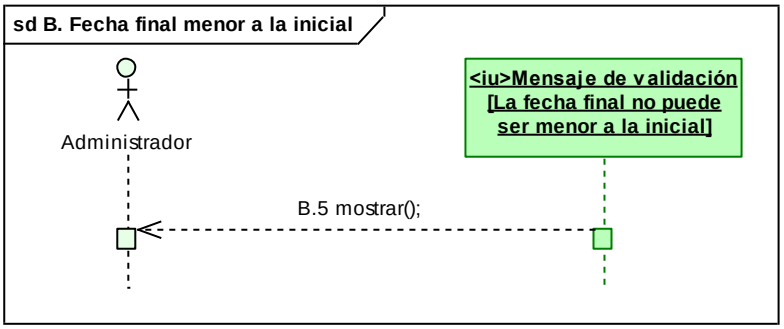


Fig.170. DS Curso Alterno: Fecha final menor a la inicial

MT34: Ver Archivos Log's

Curso Normal de Eventos

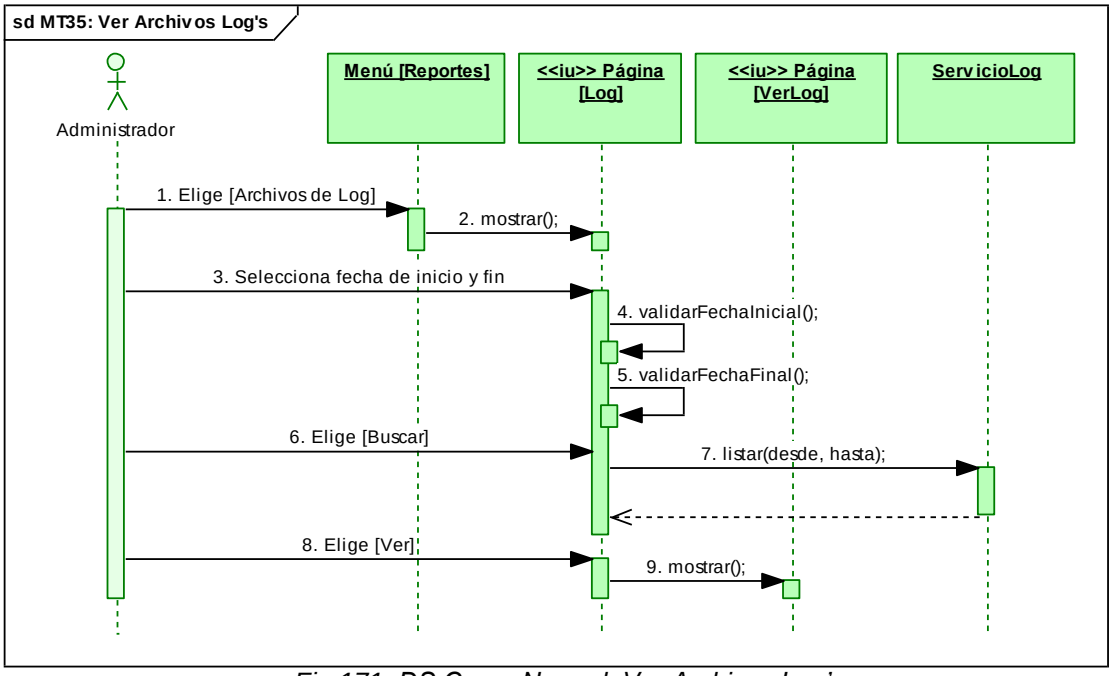


Fig.171. DS Curso Normal: Ver Archivos Log's

Cursos Alternos de Eventos

A. Fecha inicial mayor a la final

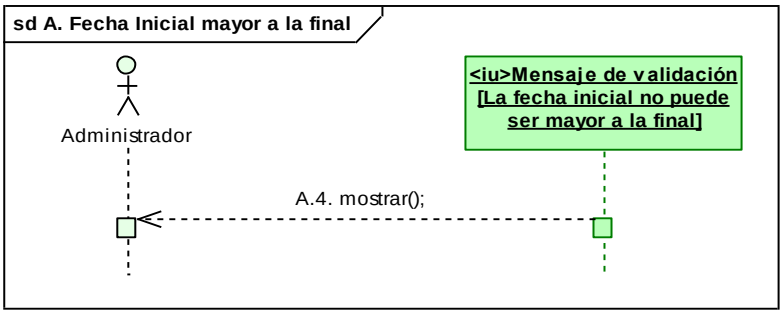


Fig.172. DS Curso Alterno: Fecha inicial mayor a la final

B. Fecha final menor a la inicial

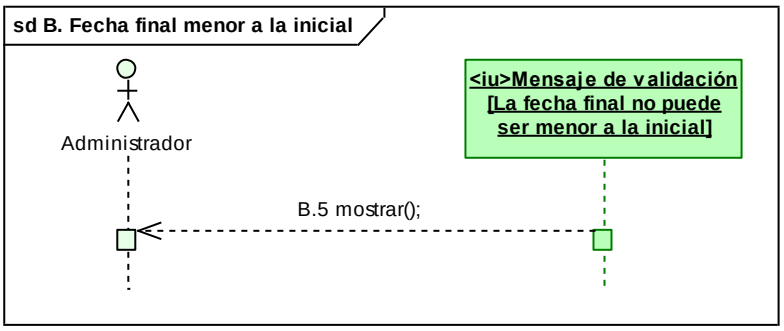


Fig.173. DS Curso Alterno: Fecha final menor a la inicial

C. Eliminar archivo log

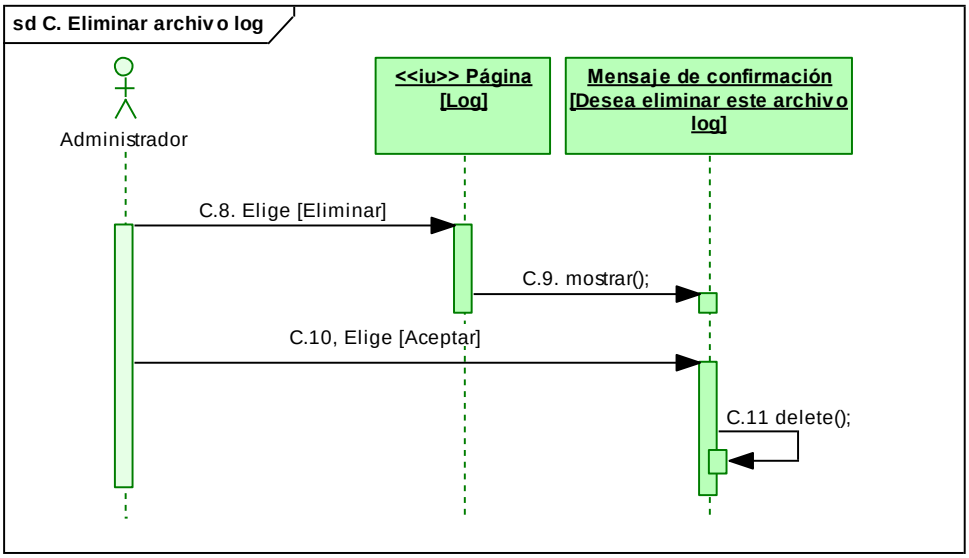


Fig.174. DS Curso Alterno: Eliminar archivo log

CASO DE USO CU010: EFECTUAR AUDITORIA

MT35: Auditar Logeo

Curso Normal de Eventos

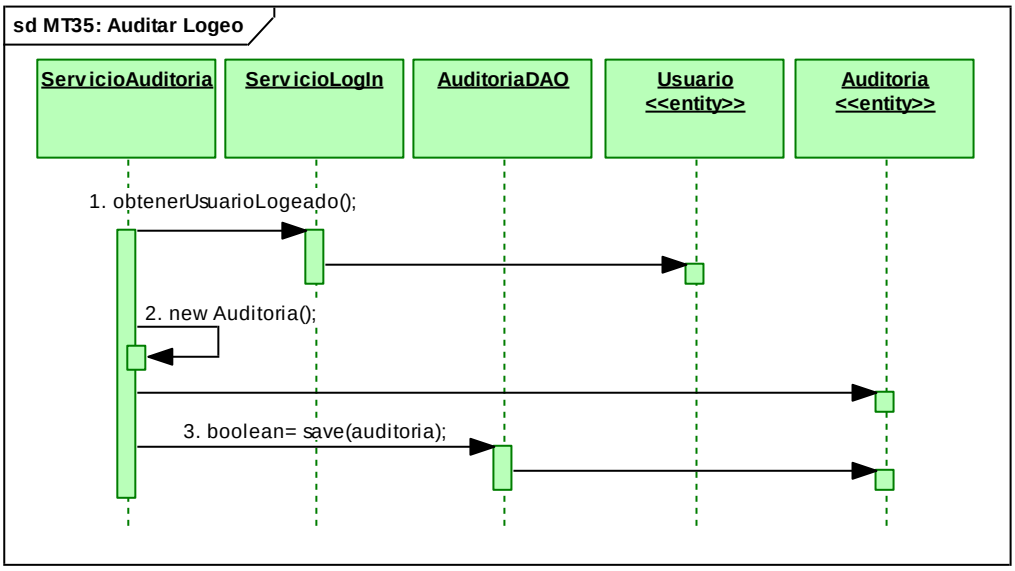


Fig.175. DS Curso Normal. Auditar Logeo

MT36: Auditar Creación de Usuario

Curso Normal de Eventos

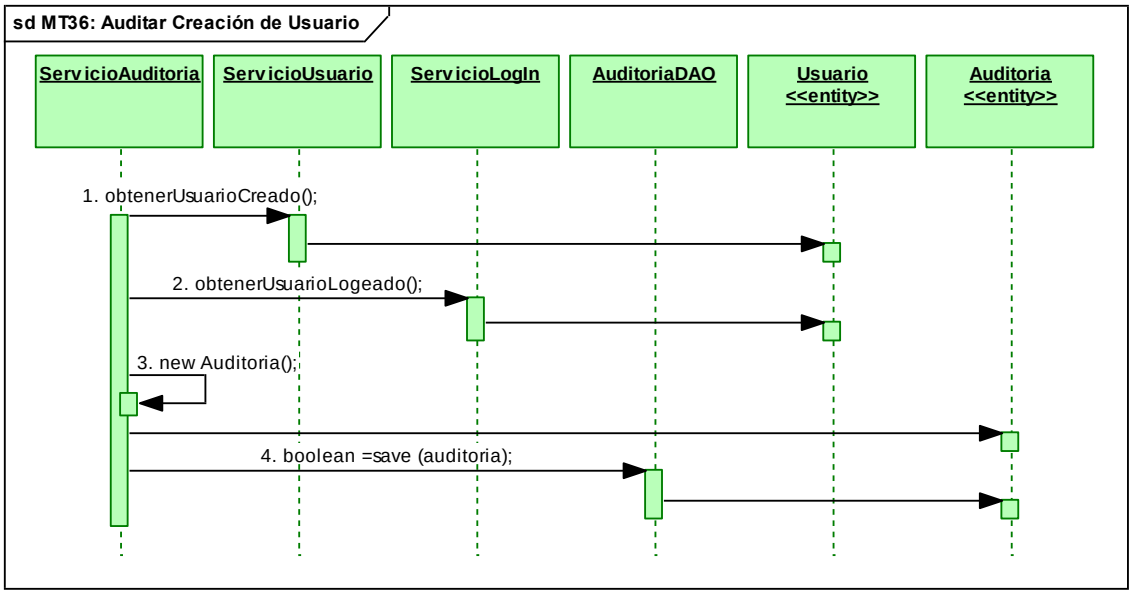


Fig.176. DS Curso Normal. Auditar Creación de Usuario

MT37: Auditar Edición de Usuario.

Curso Normal de Eventos

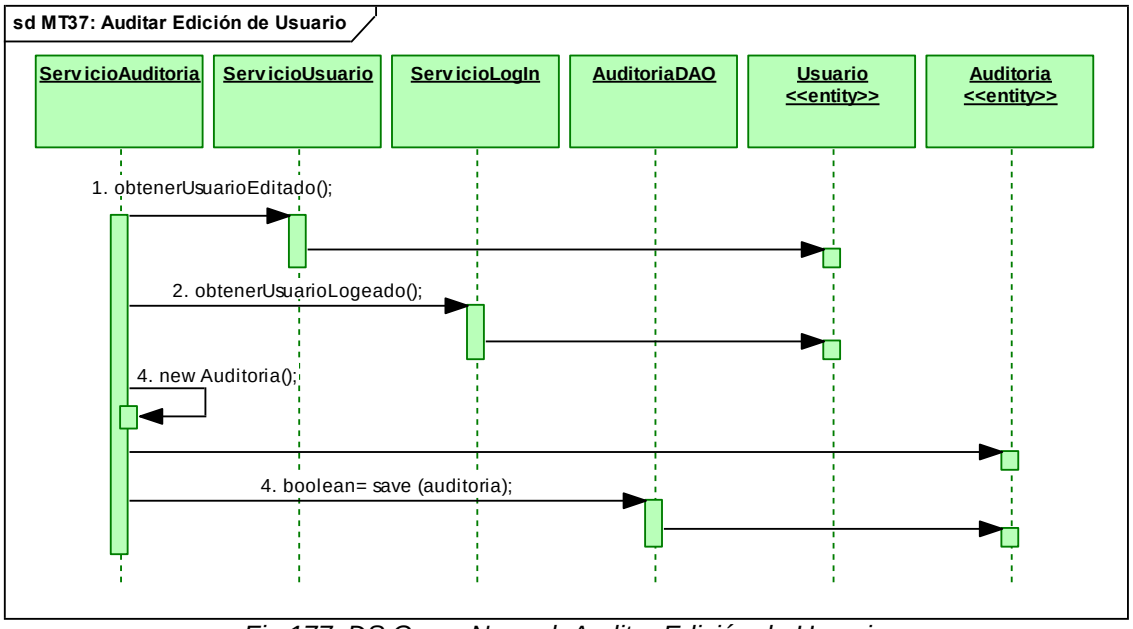


Fig.177. DS Curso Normal: Auditar Edición de Usuario

MT38: Auditar Eliminación de Usuario

Curso Normal de Eventos

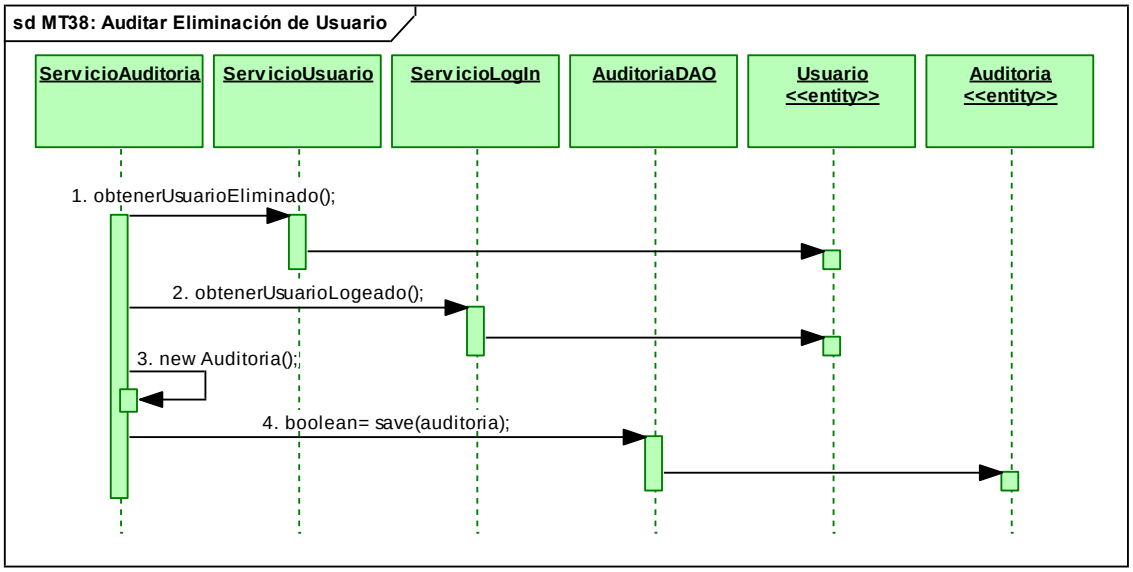


Fig.178. DS Curso Normal: Auditar Eliminación de Usuario

MT39: Auditar Creación de Certificado

Curso Normal de Eventos

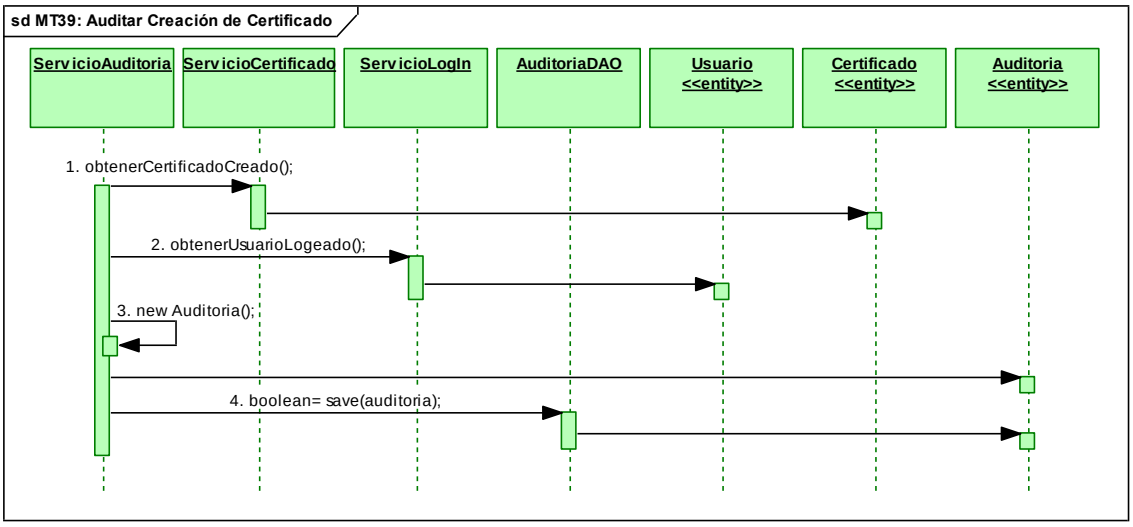


Fig.179. DS Curso Normal: Auditar Creación de Certificado

MT40: Auditar Actualización de Certificado

Curso Normal de Eventos

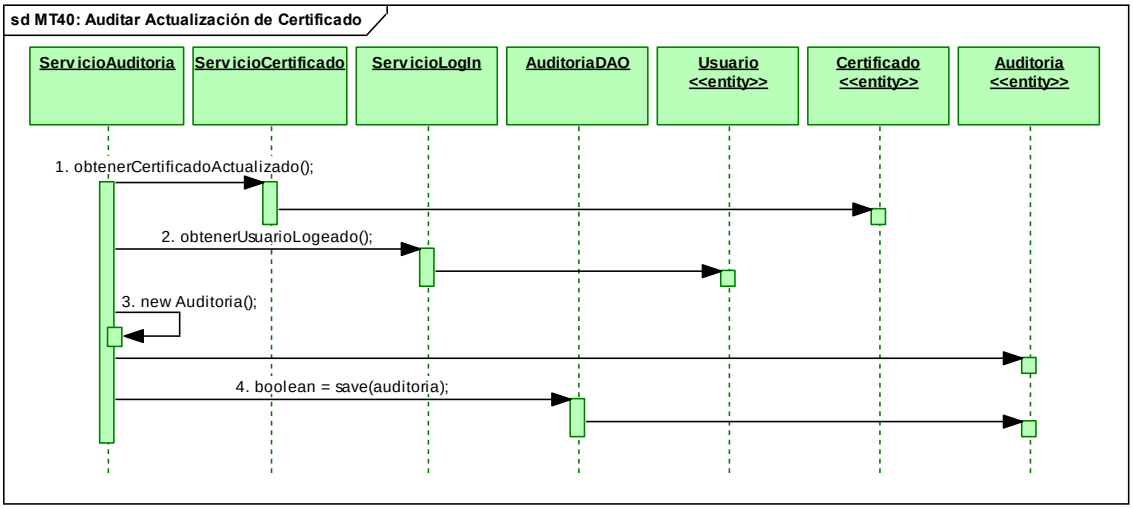


Fig.180. DS Curso Normal: Auditar Actualización de Certificado

MT41: Auditar Creación de Categoría

Curso Normal de Eventos

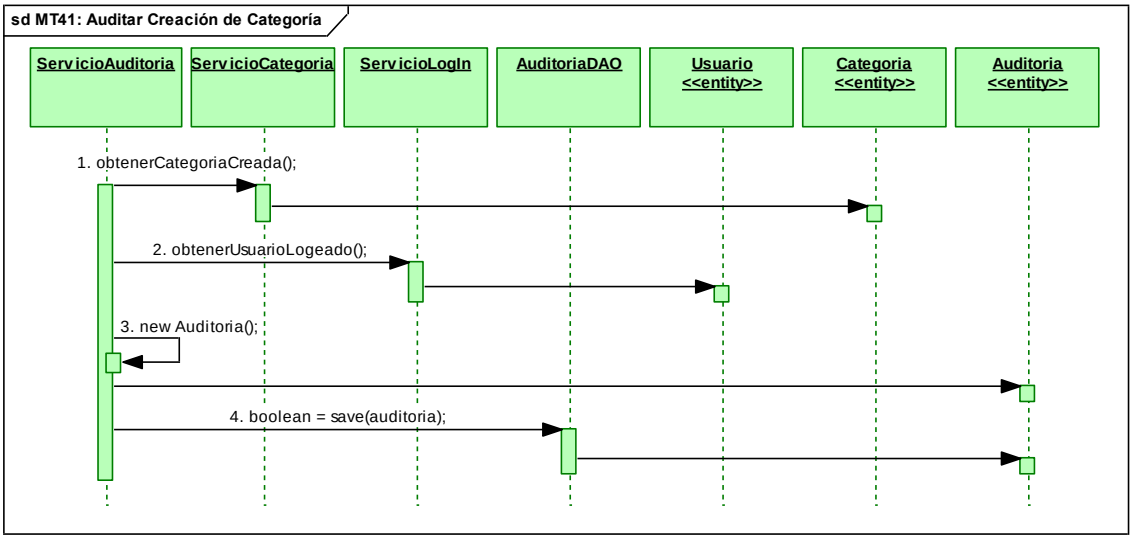


Fig.181. DS Curso Normal: Auditar Creación de Categoría

MT42: Auditar Edición de Categoría

Curso Normal de Eventos

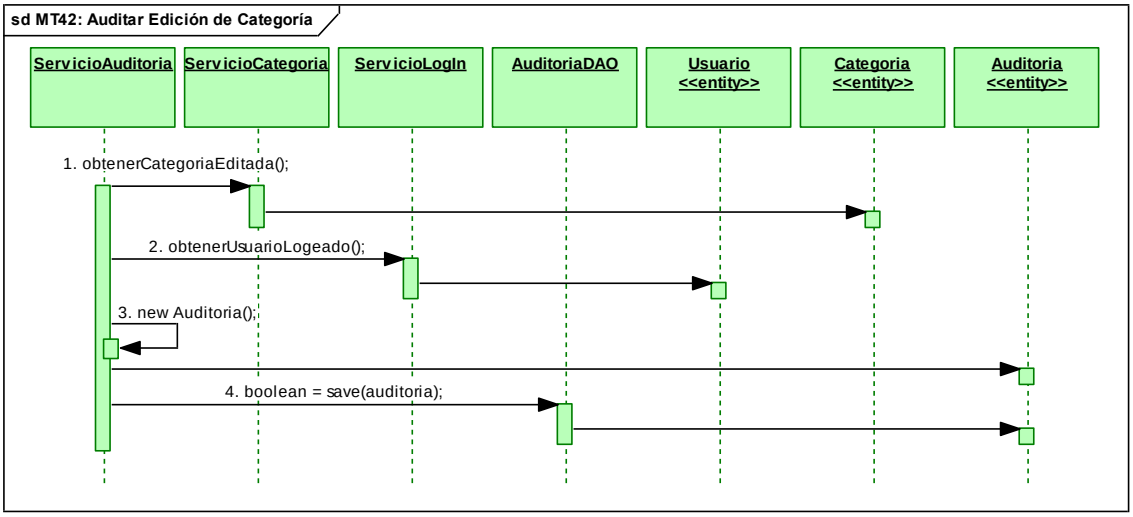


Fig.182. DS Curso Normal: Auditar Edición de Categoría

MT43: Auditar Eliminación de Categoría

Curso Normal de Eventos

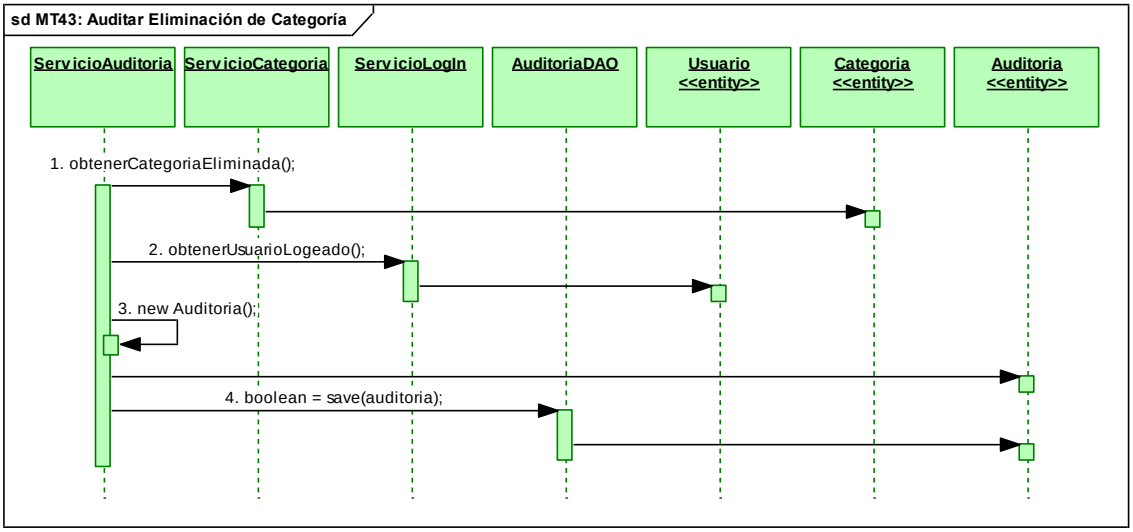


Fig.183. DS Curso Normal: Auditar Eliminación de Categoría

MT44: Auditar Creación de Plantilla

Curso Normal de Eventos

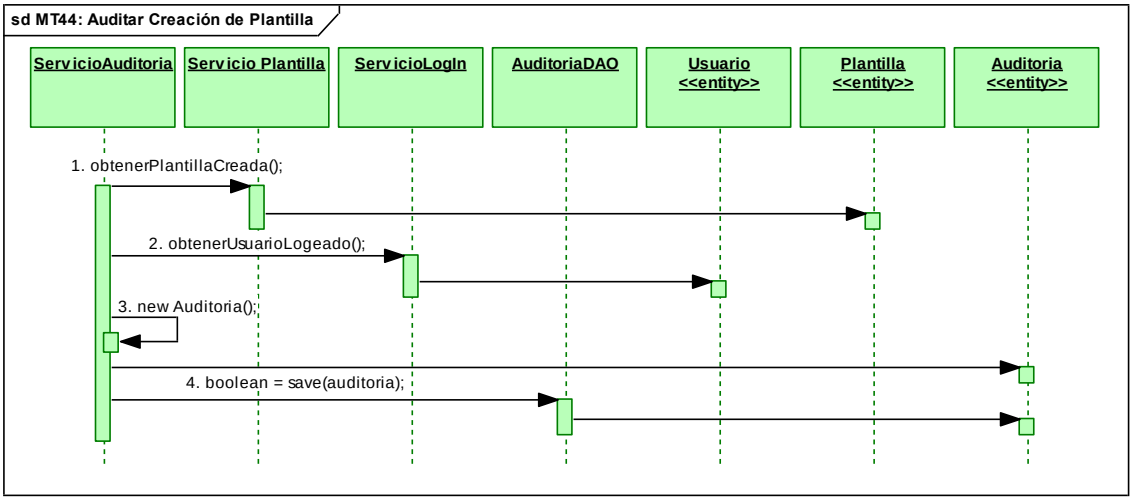


Fig.184. DS Curso Normal. Auditar Creación de Plantilla

MT45: Auditar Edición de Plantilla

Curso Normal de Eventos

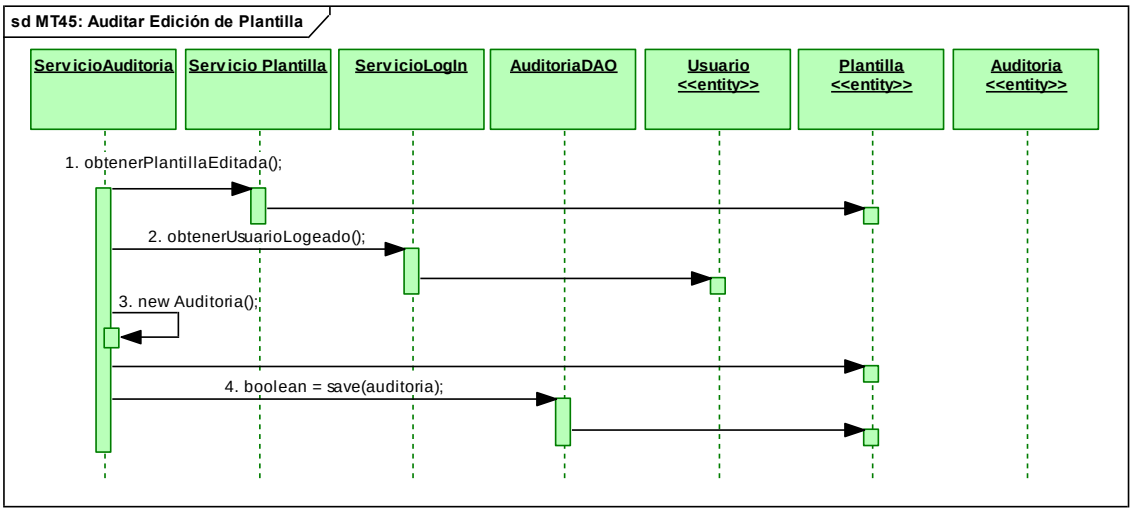


Fig.185. DS Curso Normal. Auditar Edición de Plantilla

MT46: Auditar Eliminación de Plantilla

Curso Normal de Eventos

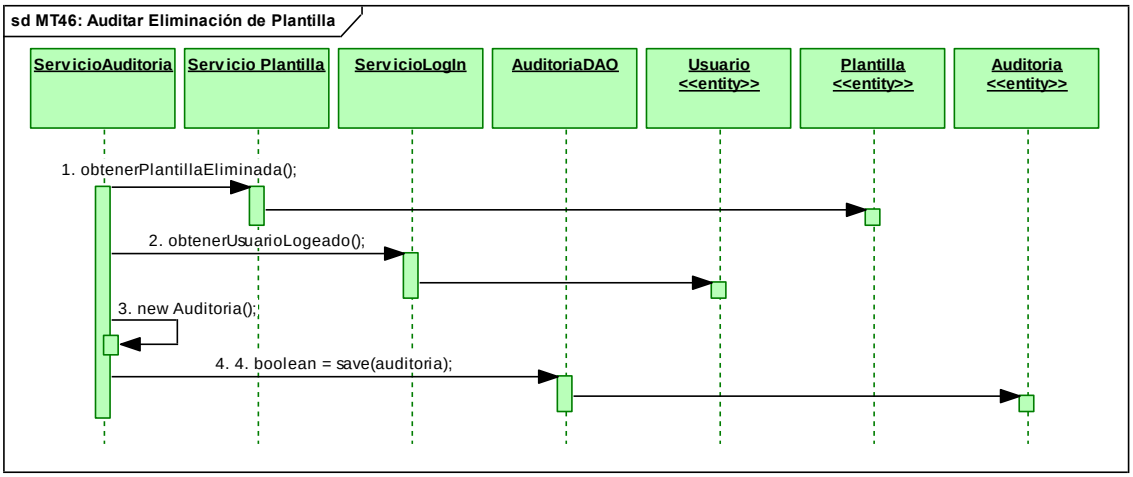


Fig.186. DS Curso Normal. Auditar Eliminación de Plantilla

MT47: Auditar Creación de Departamento

Curso Normal de Eventos

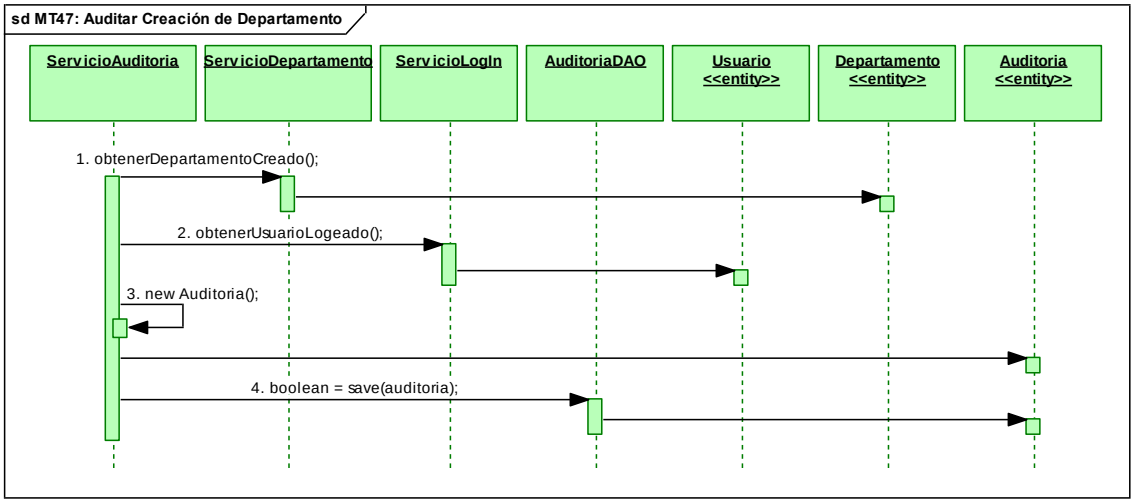


Fig.187. DS Curso Normal. Auditar Creación de Departamento

MT48: Auditar Edición de Departamento

Curso Normal de Eventos

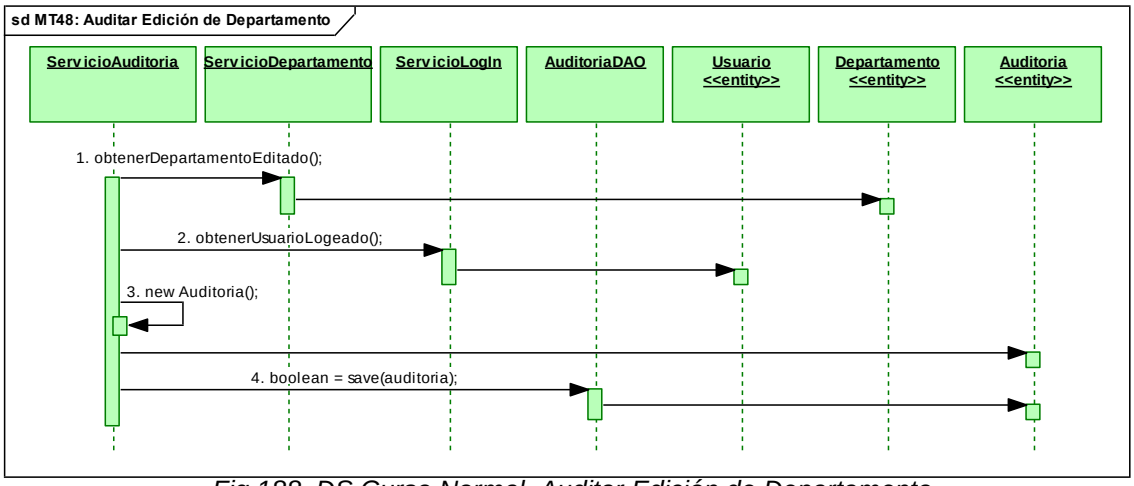


Fig.188. DS Curso Normal. Auditar Edición de Departamento

MT49: Auditar Eliminación de Departamento

Curso Normal de Eventos

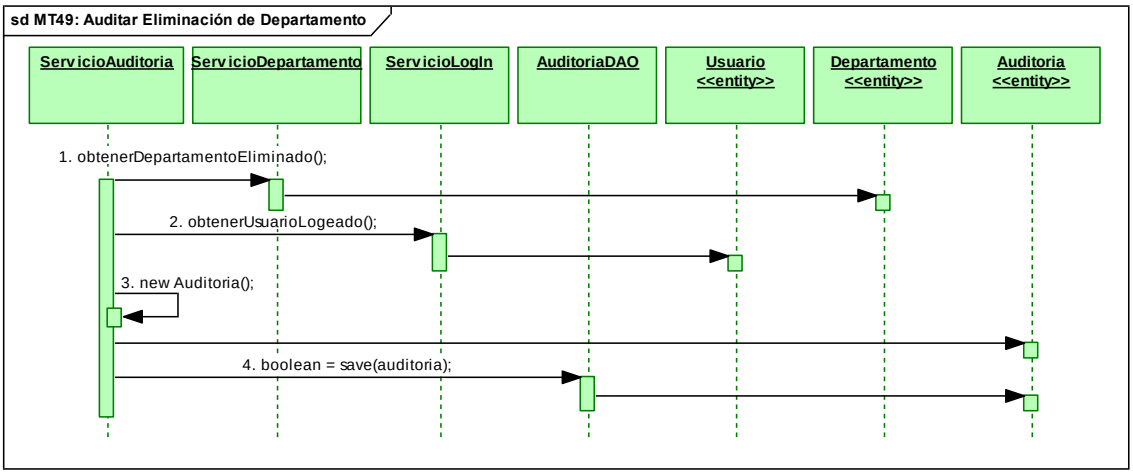


Fig.189. DS Curso Normal: Auditar Eliminación de Departamento

MT50: Auditar Edición de Parámetro

Curso Normal de Eventos

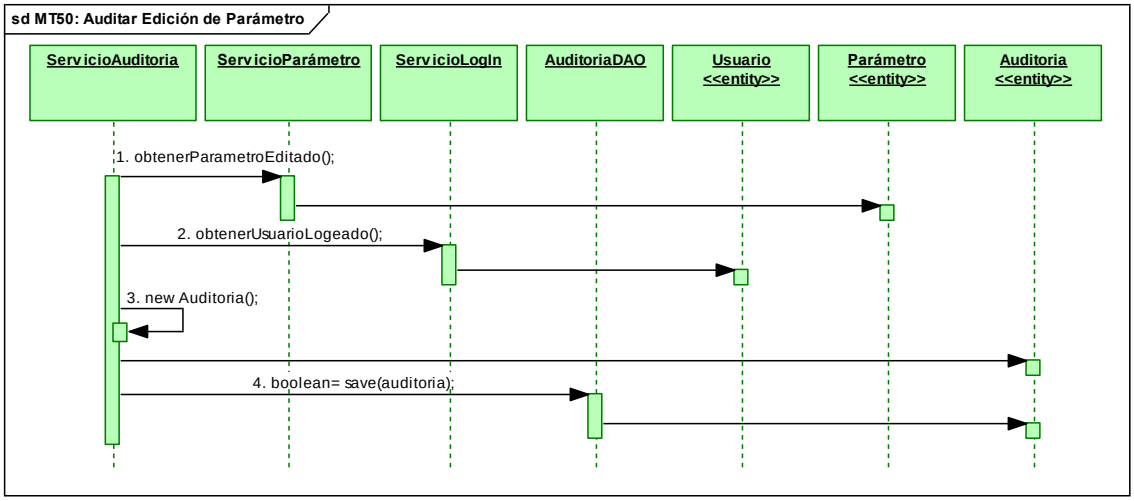


Fig.190. DS Curso Normal: Auditar Edición de Parámetro

MT51: Auditar Creación de Documento

Curso Normal de Eventos

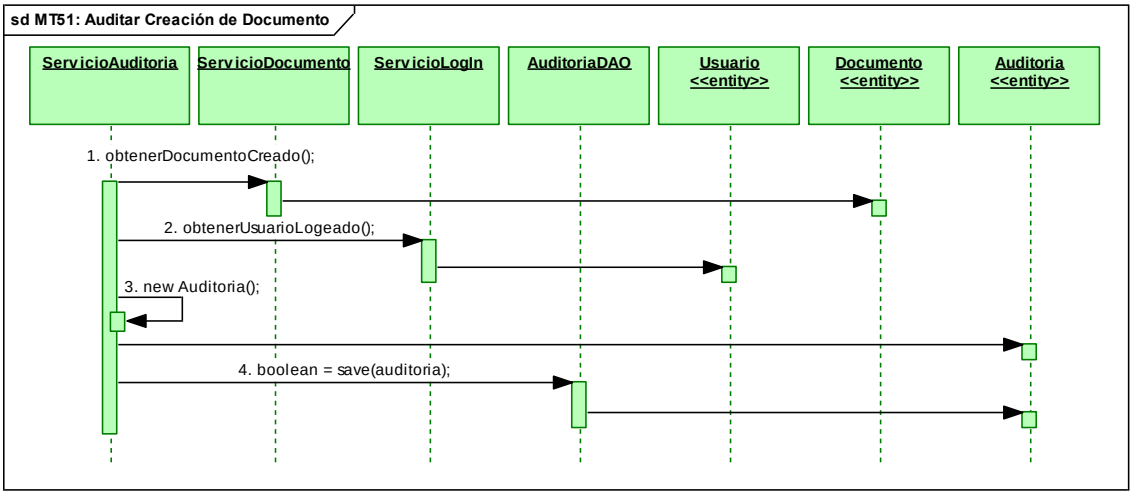


Fig.191. DS Curso Normal: Auditar Creación de Documento

MT52: Auditar Eliminación de Documento

Curso Normal de Eventos

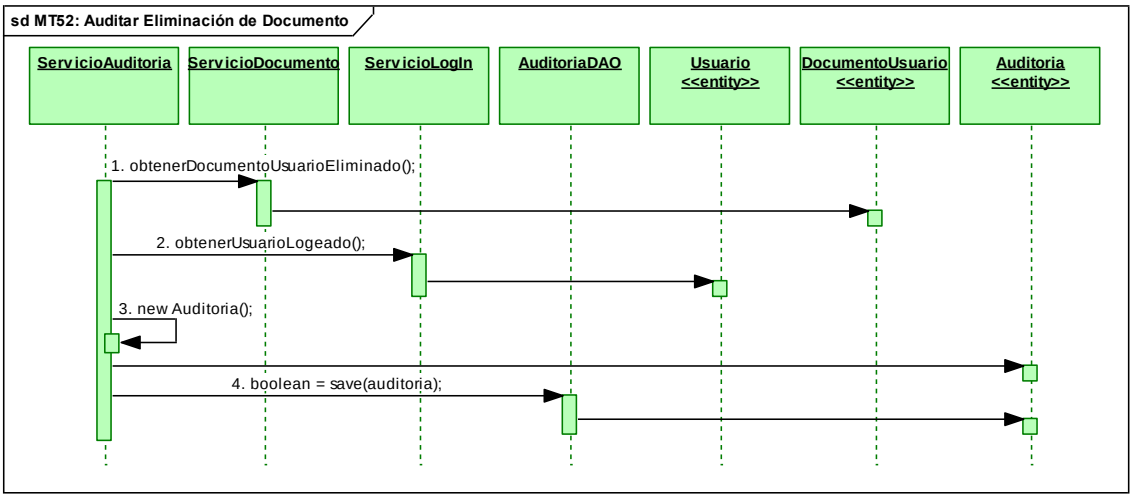


Fig.192. DS Curso Normal: Auditar Eliminación de Documento

MT53: Generar Archivos Log's

Curso Normal de Eventos

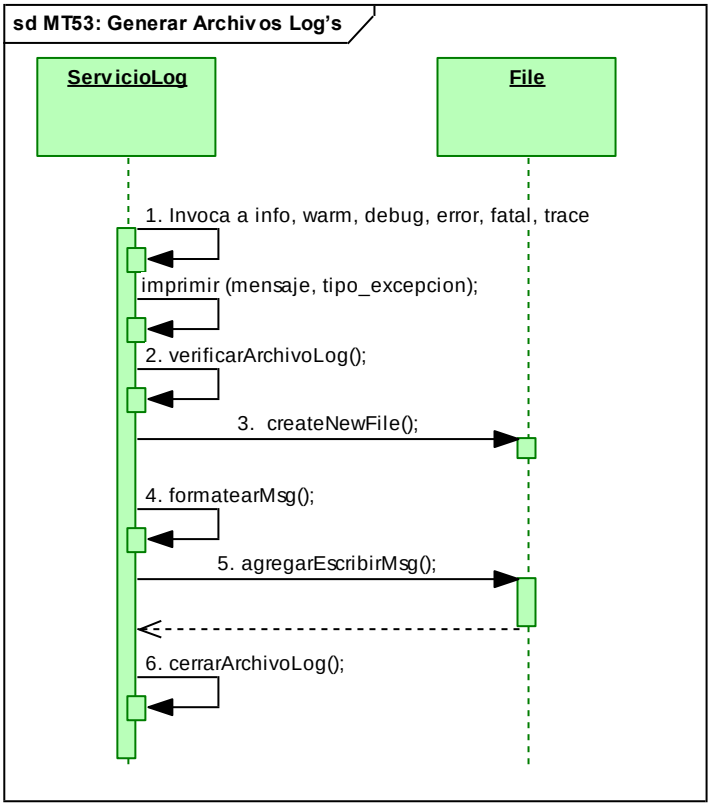


Fig.193. DS Curso Normal: Generar Archivos Log's

MT54: Buscar Respaldo

Curso Normal de Eventos

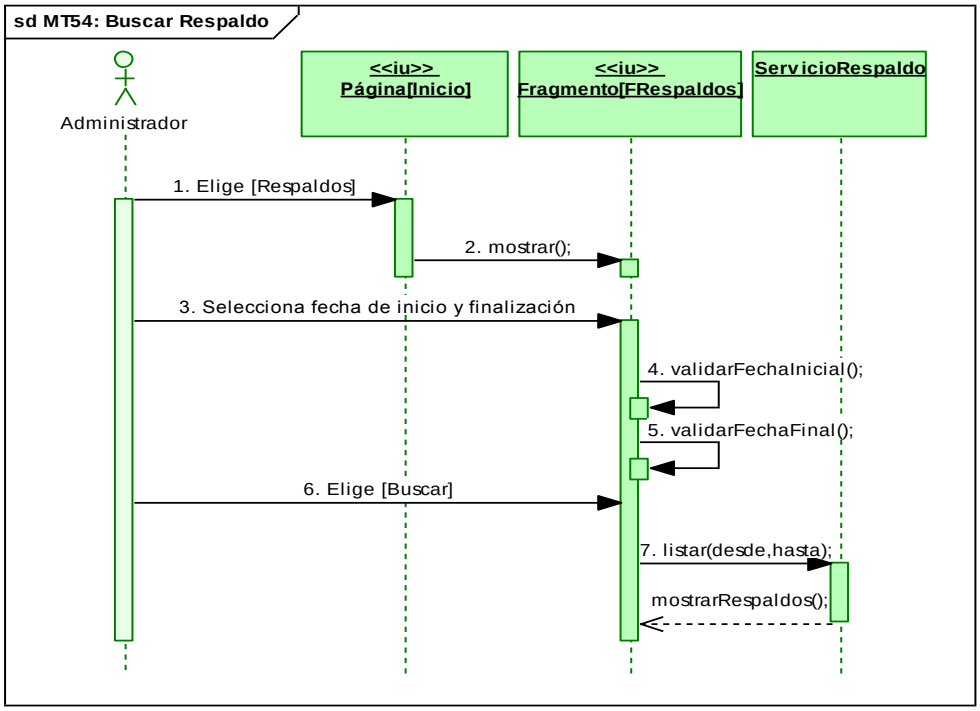


Fig.194. DS Curso Normal: Buscar Respaldo

Cursos Alternos de Eventos

A. Fecha Inicial mayor a la final

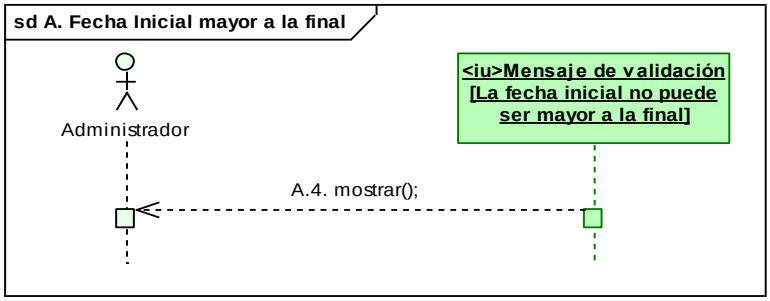


Fig.195. DS Curso Alterno: Fecha inicial mayor a la final

B. Fecha final menor a la inicial

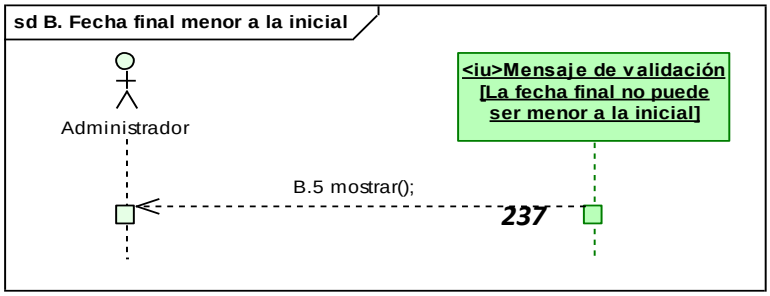


Fig.196. DS Curso Alterno: Fecha final menor a la inicial

MT55: Crear Respaldo

Curso Normal de Eventos

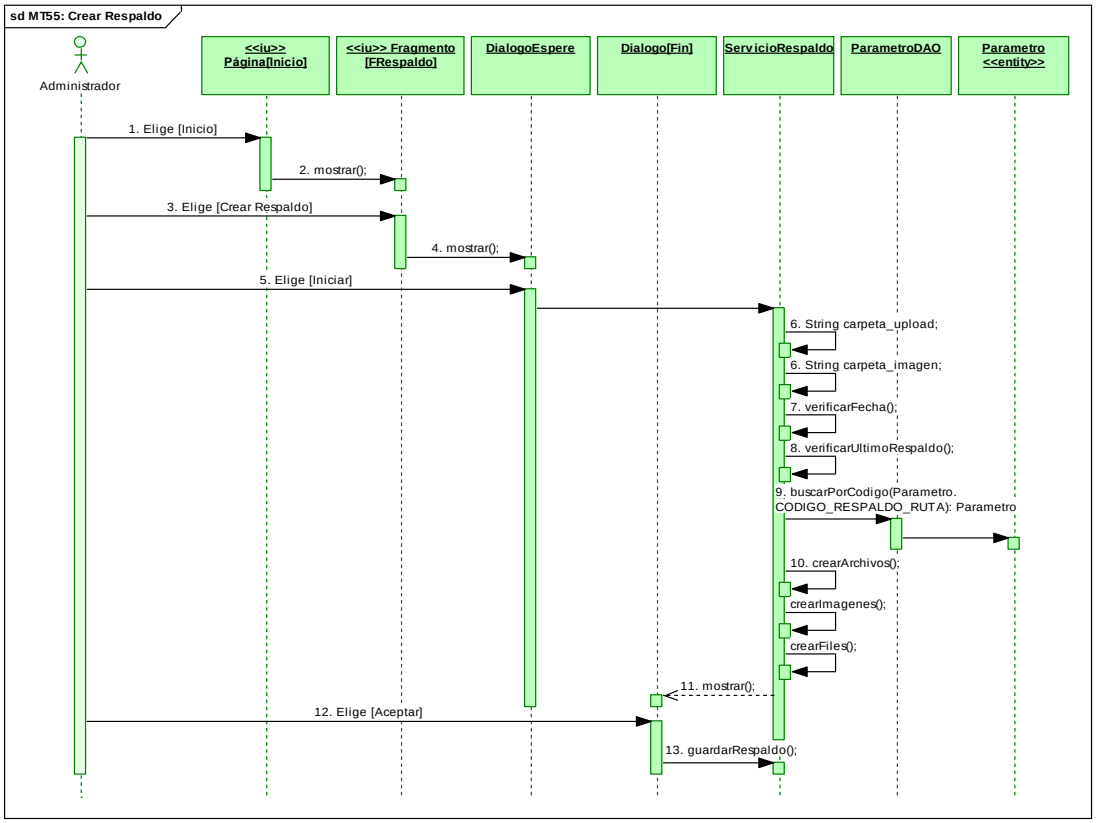


Fig.197. DS Curso Normal: Crear Respaldo

Curso Alterno de Eventos

A. Respaldo automático

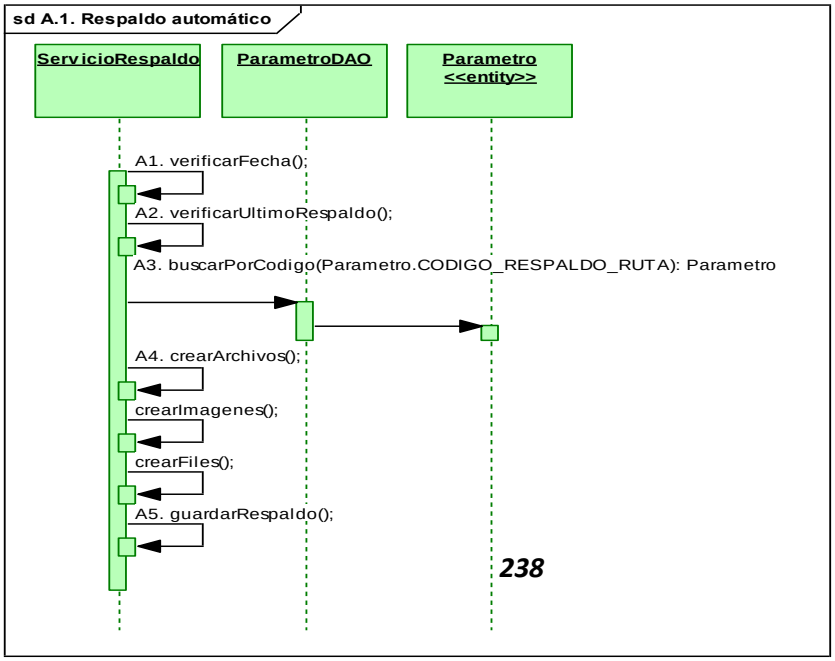


Fig.198. DS Curso Alterno: Respaldo automático

MT56 Restaurar Respaldo

Curso Normal de Eventos

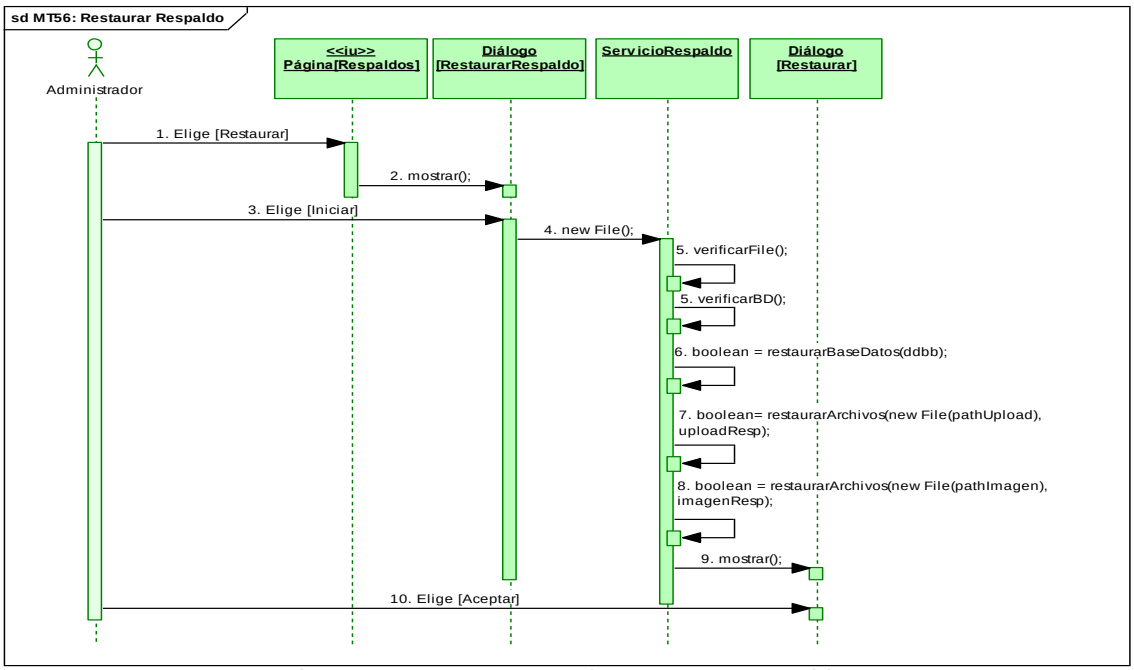


Fig.199. DS Curso Normal: Restaurar Respaldo

MT57: Eliminar Respaldo

Curso Normal de Eventos

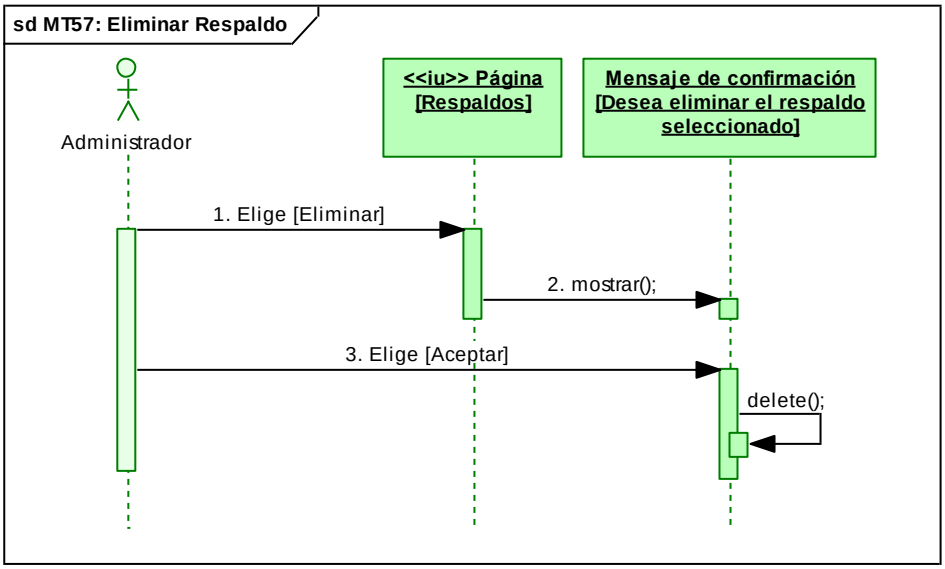


Fig.200. DS Curso Normal: Eliminar Respaldo.

8.9.2. MODELO DEL DOMINIO

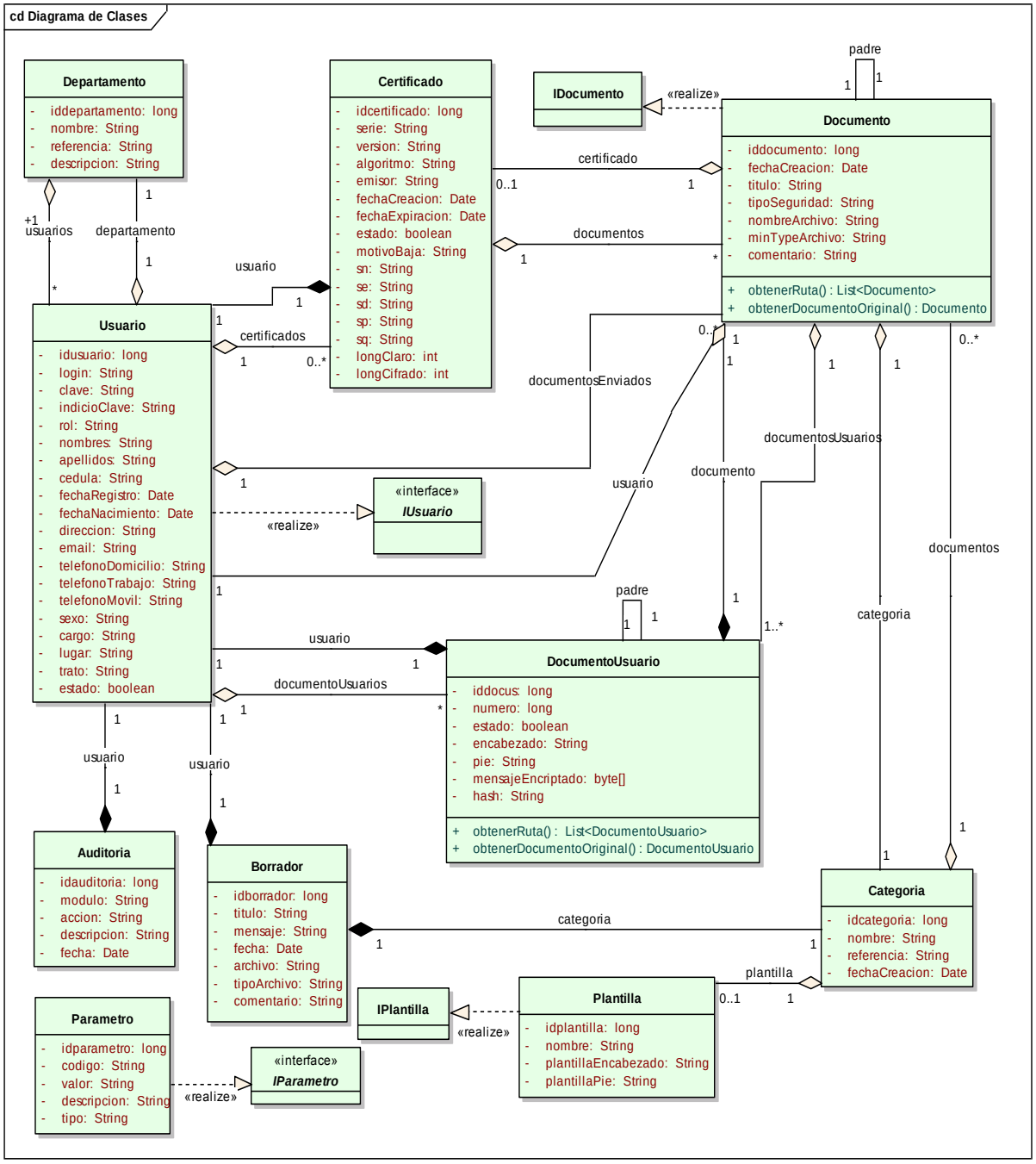


Fig.201. Modelo del Dominio

8.9.3. DIAGRAMA DE CLASES

Fig.202. Diagrama de Clases

8.9.4. MODELO CONCEPTUAL DE LA BASE DE DATOS

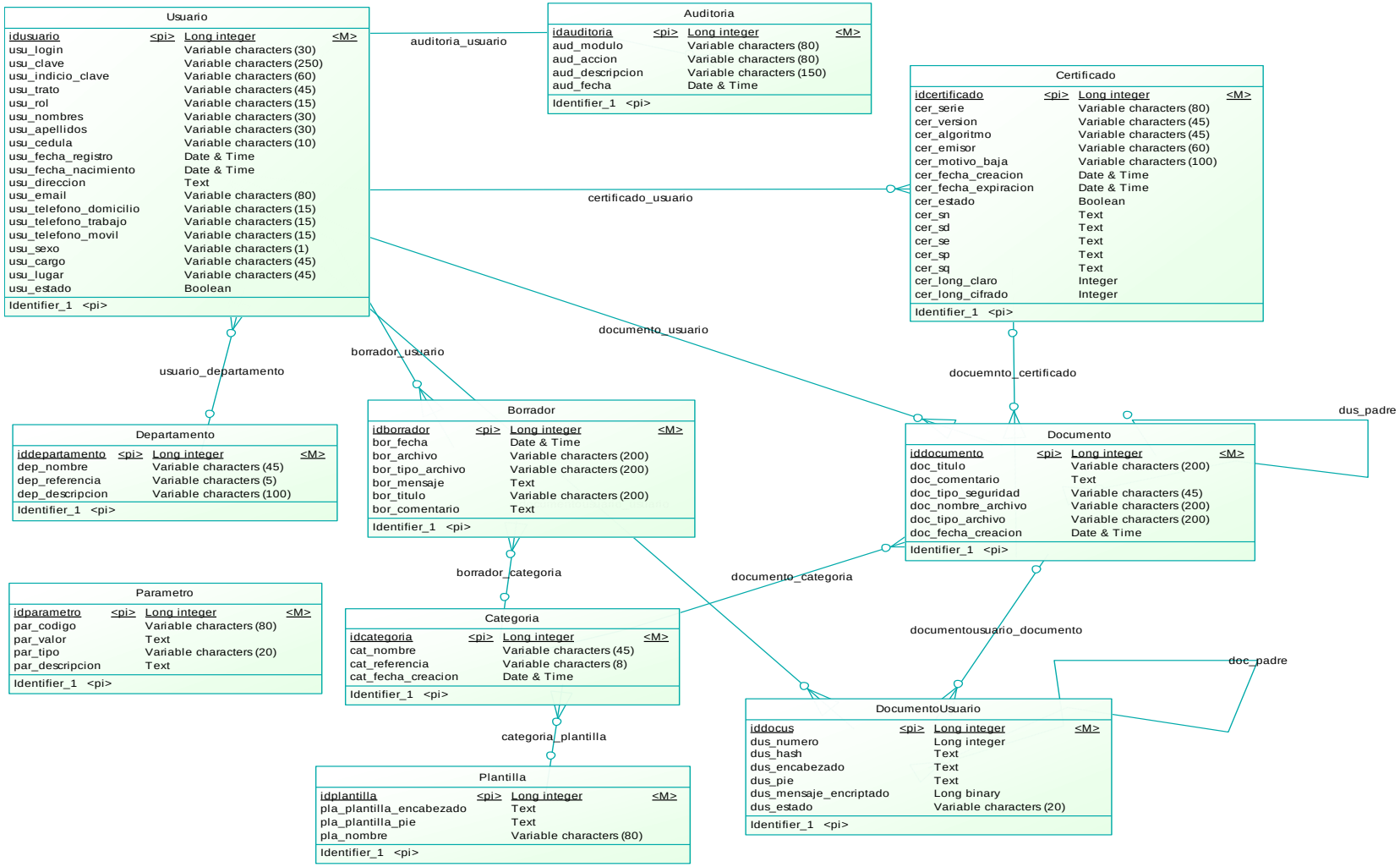


Fig.203. Modelo Conceptual de la Base de Datos

8.9.5. MODELO FÍSICO DE LA BASE DE DATOS

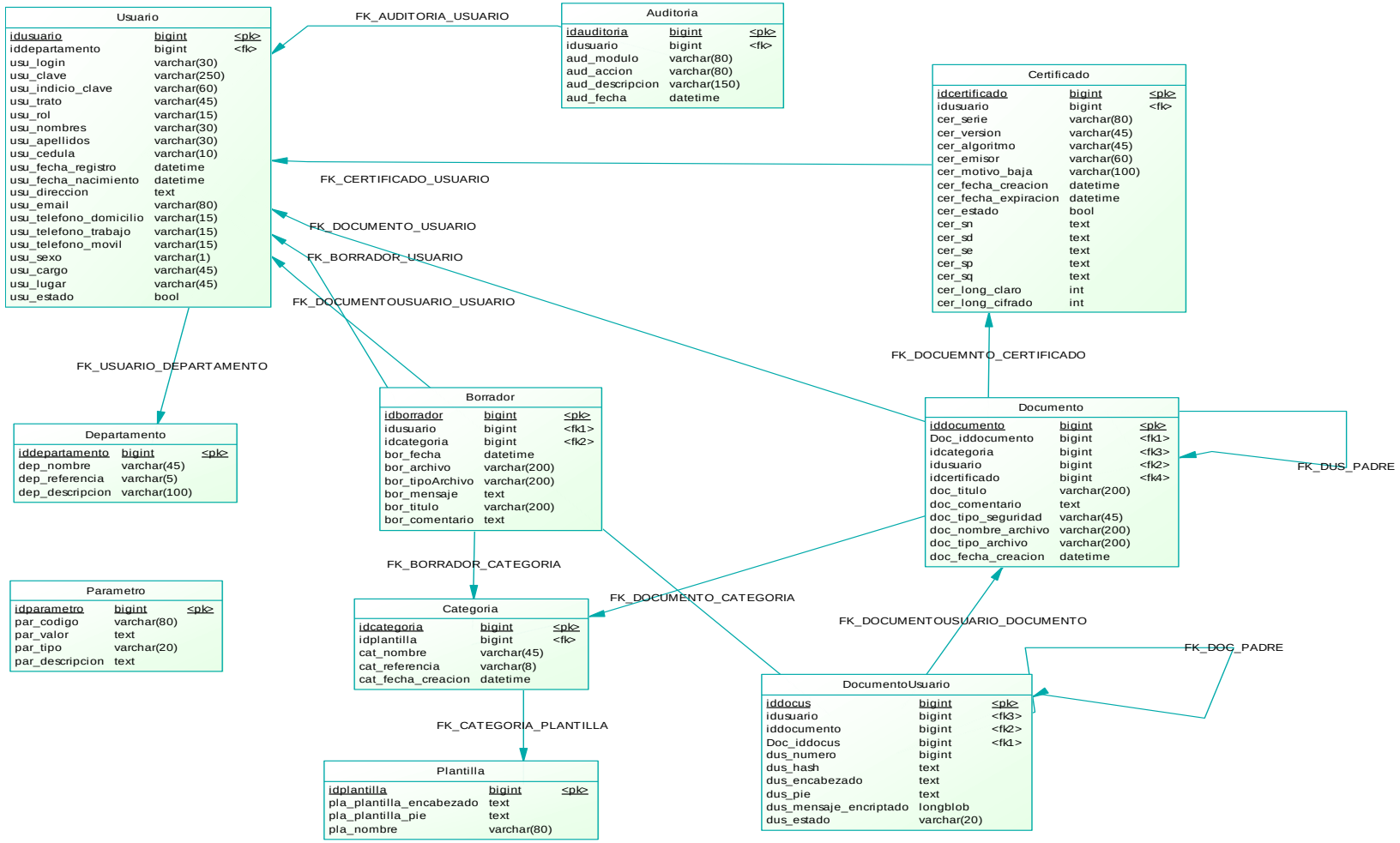


Fig.204. Modelo Físico de la Base de Datos

8.9.6. DIAGRAMA DE PAQUETES

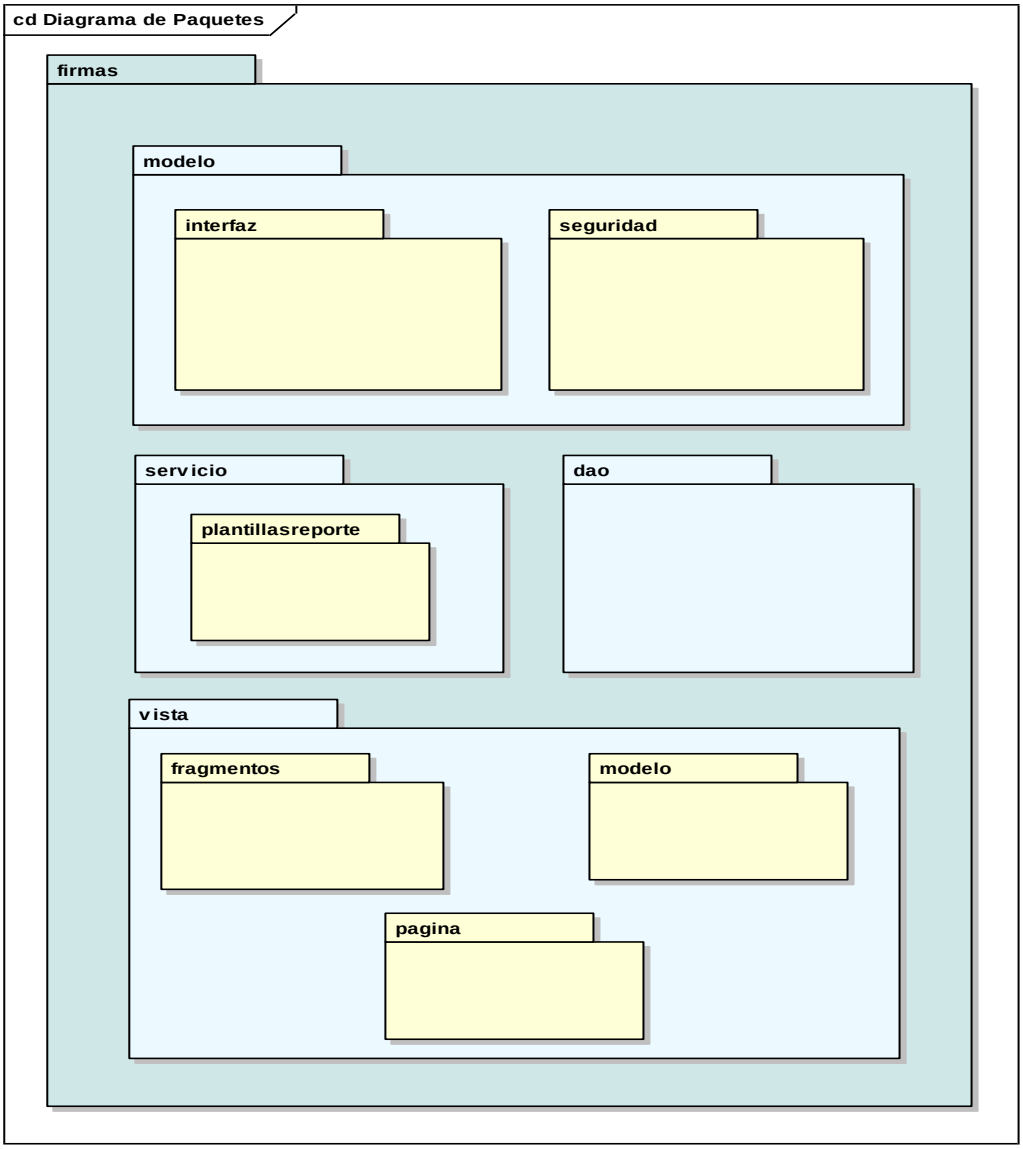


Fig.205. Diagrama de Paquetes

8.9.7. DIAGRAMA DE COMPONENTES

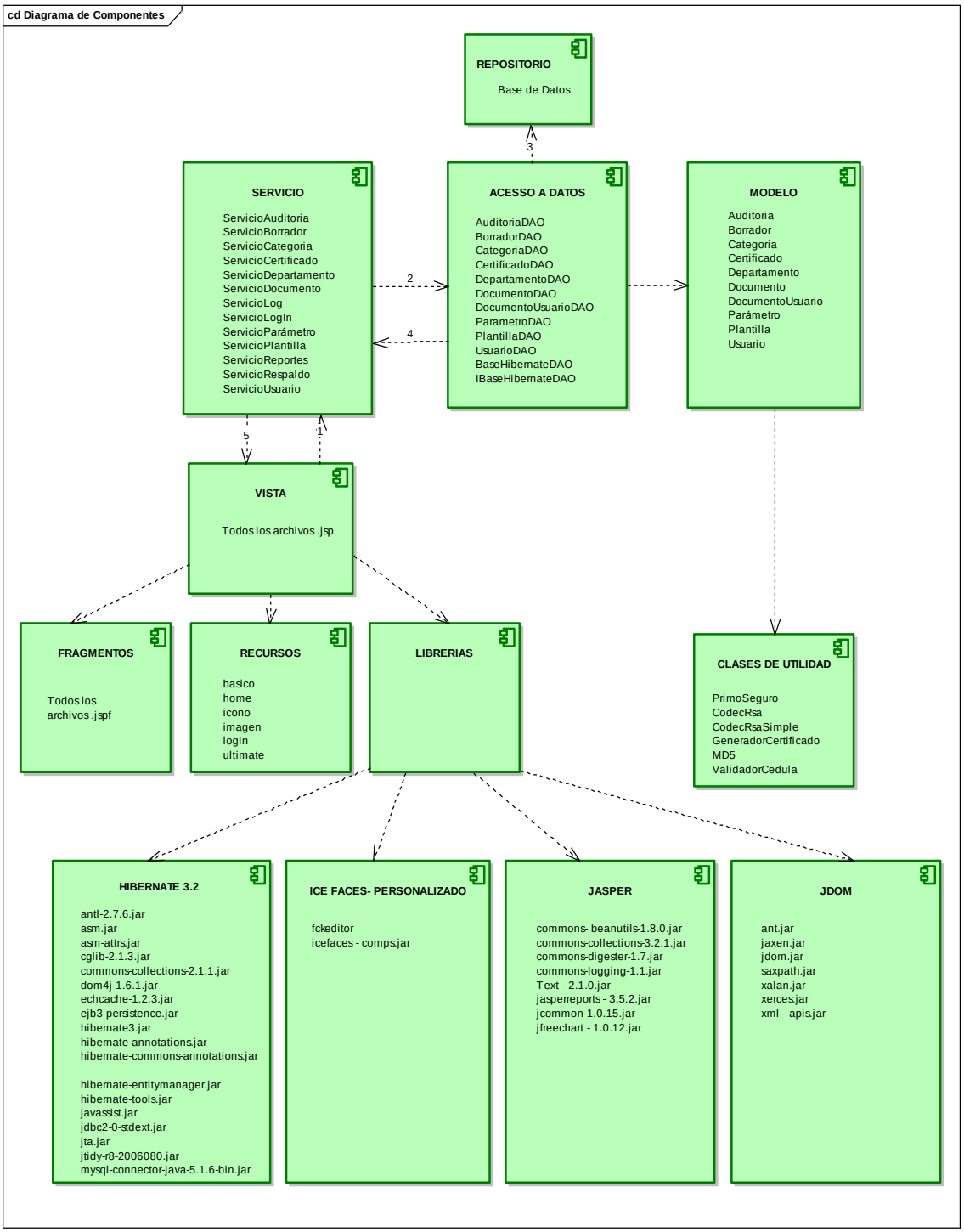


Fig.206. Diagrama de Componentes

8.9.8. DIAGRAMA DE DESPLIEGUE

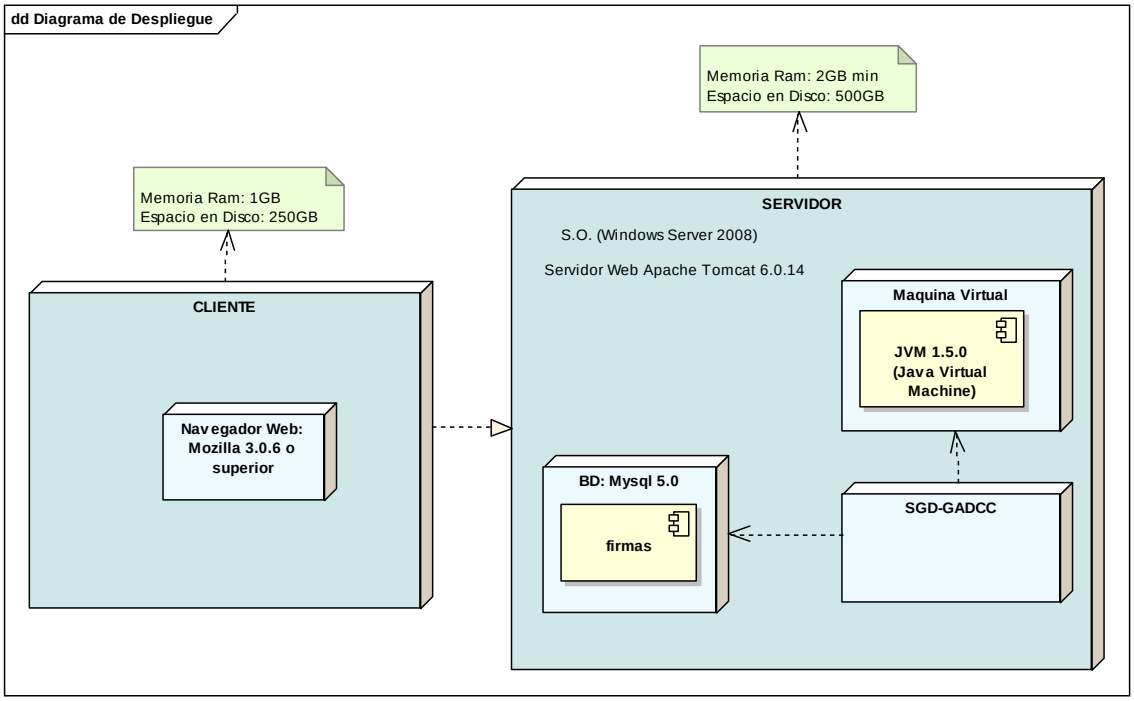


Fig.207. Diagrama de Despliegue

9. VALORACIÓN TÉCNICO ECONMÓMICA AMBIENTAL

9.1. Factibilidad Técnica

Para el desarrollo de la aplicación se contó con los recursos técnicos y tecnológicos necesarios para llevar a cabo todo este proceso. En lo que se refiere al hardware, se utilizó equipos propios, factor que fue de gran importancia, puesto que facilitó realizar la demostración piloto de cómo funcionará el sistema real en la etapa de implementación. Por su parte en lo que a recursos software se refiere, se utilizó open source (libre) debido a sus características, funcionalidades y facilidades para acceder a las mismas, es decir se optó por versiones estables con la finalidad de tener compatibilidad en toda la aplicación. A continuación se detalla las características de los equipos de desarrollo, servidor y cliente respectivamente.

Características del Equipo de Desarrollo

Hardware

Componente	Característica
Memoria RAM	1GB
Disco	250GB – 320GB
Procesador	Intel Dual Core 2.2Ghz Intel Core II Duo 2.0 Ghz

Tabla 67. Características Hardware del Equipo de Desarrollo

Software

Componente	Característica
Entorno de Programación	Java 1.5.0
Entorno de desarrollo	NetBeans 6.5
Plugin para Reportes	IReport 3.5.2 para NetBeans
Plugin para vistas	ICEFaces 1.8.1 para NetBeans
Gestor de Base de Datos	MYSQL 5.0.9
	MYSQL Front 3.2
	MYSQL Administrator 1.1
Servidor Web	Apache Tomcat 6.0.14
Herramienta de diagramación	Enterprise Architect 4.10
Sistema Operativo	Windows XP

Tabla 68. Características Software del Equipo de Desarrollo

Características del Equipo Servidor

Hardware

Componente	Característica
Memoria RAM	2GB mínimo
Disco	250GB – 320GB

Tabla 69. Características Hardware del Equipo Servidor

Software

Componente	Característica
Entorno de Programación	Java 1.5.0
Gestor de Base de Datos	MYSQL 5.0.9
Servidor Web	Apache Tomcat 6.0.14
Sistema Operativo	Windows Server 2008
Aplicación	"SGD-GADCC"

Tabla 70. Características Software del Equipo Servidor

Características del Equipo Cliente

Hardware

Componente	Característica
Memoria RAM	1GB
Disco	250 – 320

Tabla 71. Características Hardware del Equipo Cliente

Software

Componente	Característica
Navegador	Mozilla 3.0.6 o superior (recomendado)
Sistema Operativo	Windows XP/Vista/ Distribuciones Linux

Tabla 72. Características Software del Equipo Cliente

9.2. Factibilidad Operacional

El "SGD - GADCC" cumple con todos los requerimientos estimados por los usuarios. En lo que se refiere a su administración estará a cargo de un técnico en informática para atender cualquier inconveniente respecto de la misma. Por otro lado es importante recalcar que el personal que manipulará el sistema será debidamente asesorado para que de esta manera se puedan adaptar fácilmente a su uso, mismo que no se encuentra en niveles de dificultad significativos.

9.3. Factibilidad Económica

El financiamiento necesario para invertir en el desarrollo del proyecto, está determinado principalmente en los beneficios que éste aportará a la institución,

mismos que se espera sean superiores a sus costos que se incurrió al desarrollarlo. A continuación detallamos los recursos utilizados:

RECURSOS HUMANOS			
Desarrolladores			
Nombres	**Valor por hora**	**Nº de horas**	**Valor Total ($)**
Patricia Chamba	1.50	1500	2.250
Franklin Andrade	1.50	1500	2.250
Director de Tesis			
Ing. Luis Chamba	0.00	2528	0.00
Asesores			
Ing. Darwin Jiménez	0.00	500	0.00
SUBTOTAL			4.500

Tabla 73. Recursos Humanos

RECURSOS MATERIALES			
Material	**Cantidad**	**Unidad($)**	**Valor Total($)**
Anillado	10	1.00	10.00
Empastado	5	5.00	25.00
Carpetas de perfil	10	0.45	4.50
CD-R	25	0.35	8.75
Copias	2000	0.02	40.00
Grapadora	1	3.00	3.00
Grapas	2	0.50	1.00
Perforadora	1	4.00	4.00
Portaminas	2	0.70	1.40
Resma de Papel Inen A4	10	4.50	45.00
Tinta negra	10	2.70	27.00
Tinta de color	5	3.50	17.50
Infocus	4	10.00	40.00
SUBTOTAL			227.15

Tabla 74. Recursos Materiales

SERVICIOS BÁSICOS	
Servicio	**Valor Total ($)**
Luz	100.00
Teléfono	100.00
Transporte	200.00
SUBTOTAL	400.00

Tabla 75. Servicios Básicos

HARDWARE					
Equipo	**Cantidad**	**Costo($)**	**Días**	**Depreciación($)**	**Valor Total($)**
Computadora de escritorio	1	1000.00	316	365.69	634.31
Computadora de escritorio	1	800.00	316	232.71	576.29
Flash Memory	2	18.00	316	1.85	3.60
Impresoras	2	50.00	316	13.29	26.58
SUBTOTAL					1240.78

Tabla 76. Recursos Hardware

SOFTWARE	
Aplicación	**Valor Total($)**
Enterprise Architect 4.10 (Libre)	25.00
Lenguaje de Programación : JAVA Plataforma 1.5.0	0.00
Entorno de Desarrollo: NetBeans 6.5	0.00
Plugin de IReport 3.5.2 para NetBeans	0.00
Plugin ICEFaces 1.8.1 para NetBeans	0.00
Software de gestión de Bases de Datos: MYSQL 5.0.9.	0.00
MYSQL Front 3.2	0.00
MSQL Administrator 1.1	0.00
Servidor Web Apache Tomcat 6.0.14	0.00
SO: Windows XP	168.23
Herramienta para la edición: Paquete de Microsoft Office 2007	275.00
SUBTOTAL	468.23

Tabla 77. Recursos Software

COMUNICACIONES	
Medio	**Valor Total($)**
Internet	80.00
SUBTOTAL	80.00

Tabla 78. Comunicaciones

RECURSOS TÉCNICOS Y TECNOLÓGICOS	
Recurso	**Valor Total($)**
Hardware	1240.78
Software	468.23
Comunicaciones	80.00
SUBTOTAL	1709.01

Tabla 79. Recursos Técnicos y Tecnológicos

RESUMEN DE COSTOS	
Recurso	**Total ($)**
Recursos Humanos	4.500.00
Recursos Materiales	227.15
Servicios Básicos	400.00
Comunicaciones	80.00
Recursos Técnicos y Tecnológicos	1709.01
SUBTOTAL	6.916.16
IMPREVISTOS (5%)	345.80
TOTAL	7.261.96

Tabla 80. Resumen de Costos

10. PRUEBAS Y VALIDACIÓN

El presente plan de validación para el Sistema de Gestión Documental en el Municipio de Calvas se realizó los días 24, 25 y 26 de Mayo del año en curso, en dicha prueba se distribuyó la funcionalidad del sistema de acuerdo a los roles de usuario y de administrador, definiendo para ello a 4 administradores y a 10 usuarios respectivamente. El Analista de Sistemas de la institución fue quién se encargó de verificar que todo este proceso se cumpla satisfactoriamente (Ver Anexo 5)

Las pruebas en el sistema se efectuaron con la finalidad de verificar el grado de funcionalidad y aceptación que dicho producto tuvo por parte de los usuarios. Para conseguir este propósito se creyó conveniente distribuir las pruebas en tres tipos: pruebas de funcionalidad, pruebas de aceptación y pruebas de usabilidad. En lo referente a las encuestas, éstas se dirigieron tanto para administradores como para usuarios (Ver Anexo 4).

Cabe indicar que en el caso de administradores, éstos fueron capaces de valorar el sistema en los módulos de usuario, certificado, categoría, departamento, plantilla, parámetro, documento y respaldos. En el caso de usuarios ellos solamente valoraron el módulo de documentos.

10. 1. TIPOS DE PRUEBA

Prueba de funcionalidad.- Pruebas destinadas a verificar que el sistema cumpla con los requerimientos definidos en la etapa de análisis; es decir comprobar funciones correctas o ausentes tanto en la interfaz gráfica como en la base de datos. Algunos de los procesos que se evaluaron fueron:

- ☞ Creación de usuarios, categorías, departamentos, plantillas y documentos.
- ☞ Edición de usuarios, categorías, departamentos, plantillas y documentos.
- ☞ Eliminación de usuarios, categorías, departamentos, plantillas y documentos.
- ☞ Envío y recepción de documentos

Prueba de aceptación.- Pruebas encargadas de verificar la funcionalidad total de la aplicación, así como también comprobar el nivel de satisfacción existente por parte usuarios y administradores. Para valorar estas pruebas se efectúo encuestas, en las cuales dichos resultados demostraron que la aplicación si cumple con todos los requerimientos planteados.

Pruebas de usabilidad.- Pruebas encargadas de evaluar la utilidad y robustez del sistema en lo que se refiere a interfaz gráfica, facilidad de navegación, consulta, y de generación de reportes.

Para verificar los resultados de las pruebas indicadas anteriormente se creyó conveniente utilizar un esquema de niveles para cada acreditación; dicho esquema es el siguiente:

- ☞ *Excelente*
- ☞ *Muy Bueno*
- ☞ *Bueno*
- ☞ *Regular*

Las funcionalidades que se calificaron fueron las que a continuación detallamos:

Para el administrador

- ✓ Rapidez en el acceso
- ✓ Seguridad en el acceso
- ✓ Interfaz amigable
- ✓ Información de ayuda
- ✓ Ingreso de datos
- ✓ Validación de Datos
- ✓ Módulos que cuenta la aplicación
- ✓ Funcionalidades de cada módulo
- ✓ Búsqueda y organización de la información
- ✓ Rapidez en el envió de mensajes
- ✓ Rapidez en la recepción de mensajes
- ✓ Almacenamiento y recuperación de la información
- ✓ Utilización de certificados digitales en el envío y recepción de mensajes
- ✓ Ruta o seguimiento de la información
- ✓ Uso de plantillas para la creación de documentos
- ✓ Listado y generación de reportes
- ✓ Parametrización en el sistema
- ✓ Respaldos automáticos y manuales
- ✓ Sintaxis y referencias de categorías y departamentos

Para el usuario

- ✓ Rapidez en el acceso
- ✓ Interfaz amigable y ambiente de trabajo
- ✓ Colores utilizados
- ✓ Tamaño y tipo de letra
- ✓ Representación de resultados en tablas
- ✓ Pautas e información de ayuda
- ✓ Imágenes utilizadas en el sistema
- ✓ Información del municipio
- ✓ Búsqueda y recuperación de la información
- ✓ Organización de la información
- ✓ Creación de documentos
- ✓ Rapidez en el envió de documentos
- ✓ Lectura y almacenamiento de la información
- ✓ Utilización de certificados digitales en el envío y recepción de mensajes
- ✓ Ruta o seguimiento de la información

10.2. RESULTADOS DE VALIDACIÓN

Luego de efectuar las encuestas, se procedió a tabular dichos resultados, (Ver Anexo 6) los cuales permitieron en lo posterior calificar el nivel de aceptación que tiene la aplicación. Los resultados de validación fueron:

Funcionalidad	Rango			
	Excelente	Muy Bueno	Bueno	Regular
1.Rapidez en el acceso	*1*	*3*	-	
2.Seguridad en el acceso	*2*	*2*	-	
3.Interfaz amigable	*0*	*4*	-	
4. Información de ayuda	*0*	*4*	-	
5. Ingreso de datos	*1*	*3*	-	
6. Validación de Datos	*1*	*3*	-	
7. Módulos que cuenta la aplicación	*1*	*2*	*1*	
8. Funcionalidades de cada módulo	*0*	*4*	-	
9. Búsqueda y organización de la información	*1*	*3*	-	
10. Rapidez en el envió de mensajes	*1*	*3*	-	
11. Rapidez en la recepción de mensajes	*1*	*3*	-	
12. Almacenamiento y recuperación de la información	*1*	*3*	-	
13. Utilización de certificados digitales en el envío y recepción de mensajes	*1*	*3*	-	
14. Ruta o seguimiento de la información	*1*	*2*	*1*	
15. Uso de plantillas para la creación de documentos	*0*	*3*	*1*	
16. Listado y generación de reportes	*0*	*4*	*0*	
17. Parametrización en el sistema	*0*	*3*	*1*	
18. Respaldos automáticos y manuales	*0*	*2*	*2*	
19. Sintaxis y referencias de categorías y departamentos	*0*	*4*	-	
TOTAL	*12*	*58*	*6*	

Tabla 81. Resultados de validación rol Administrador

Funcionalidad	Rango			
	Excelente	**Muy Bueno**	**Bueno**	**Regular**
Rapidez en el acceso	*2*	*8*	-	
Interfaz amigable y ambiente de trabajo	*3*	*7*	-	
Colores utilizados	*2*	*6*	*2*	
Tamaño y tipo de letra	*2*	*6*	*2*	
Representación de resultados en tablas	*0*	*9*	*1*	
Pautas e información de ayuda	*4*	*3*	*3*	
Imágenes utilizadas en el sistema	*0*	*8*	*2*	
Información del municipio	*0*	*7*	*3*	
Búsqueda y recuperación de la información	*0*	*10*	*0*	
Organización de la información	*1*	*9*	*0*	
Creación de documentos	*1*	*7*	*2*	
Rapidez en el envió de documentos	*3*	*6*	*1*	
Lectura y almacenamiento de la información	*1*	*9*	*0*	
Utilización de certificados digitales en el envío y recepción de mensajes	*6*	*4*	*0*	
Ruta o seguimiento de la información	*3*	*6*	*1*	
TOTAL	*28*	*105*	*17*	

Tabla 82. Resultados de validación rol Usuario

Los resultados de las pruebas realizadas al “SGD- GADCC”, en su mayoría estuvieron estipulados en los niveles de Muy Bueno y Excelente según criterio de Administradores y Usuarios encuestados. Cabe recalcar que existieron al inicio algunas dificultades para la manipulación del sistema, esto debido a que el proceso de firma de documentos, requiere el uso de claves públicas y privadas, y básicamente es un proceso nuevo que ningún usuario antes había utilizado. Por ello es que en vista de aquello, una vez que el sistema se implemente, se cree necesario el asesorar y capacitar suficientemente al personal de la institución en el manejo adecuado de todas las funcionalidades de la aplicación y evitar posteriores inconvenientes.

10.3. CONTROL DE CALIDAD EN LA APLICACIÓN

La obtención de un software con calidad implica la utilización de metodologías o procedimientos estándares para el análisis, diseño, programación y prueba del software que permitan uniformar la filosofía de trabajo, con la finalidad de lograr una mayor confiabilidad, mantenibilidad y facilidad de prueba, a la vez que eleven la productividad, tanto para la labor de desarrollo como para el control de la calidad del software.

Por ello, es que para determinar la calidad en nuestra aplicación creímos conveniente definir algunos parámetros que fueron modificados, creados o en su caso eliminados, orientándonos siempre por lograr cumplir a cabalidad con los requerimientos definidos en la etapa de análisis por parte del cliente, así como también el proporcionar un software que se adapte fácilmente a quienes lo van a manipular.

Los parámetros que elegimos para efectuar el control de calidad están estimados en base a cada módulo, y a la interfaz gráfica que rodea el sistema. A continuación en la siguiente tabla se muestra en forma detallada dichos aspectos:

Nombre del Módulo	Parámetro Anterior	Parámetro Actual	Observación
Sistema	**Log In**: Parámetro utilizado para que cada usuario tenga acceso al sistema, de acuerdo a su contraseña previamente asignada.	*Iniciar Sesión*	*Cambio de nombre a parámetro*
	Log Off: Parámetro utilizado para finalizar o cerrar una sesión de un usuario en el sistema.	*Cerrar Sesión*	*Cambio de nombre a parámetro*
		Contador de Intentos para Ingresar al sistema	*Parámetro nuevo*
		Indicio para recordar clave de acceso al sistema	*Parámetro nuevo*
		Verificador de acceso al sistema que evite que un mismo usuario pueda logearse más de una vez al mismo tiempo	*Parámetro nuevo*
Usuario	**Us:** Parámetro utilizado para identificar a cada usuario que ha iniciado sesión	*Usuario*	*Cambio de nombre a parámetro*
		Validador de cada campo, que permita saber cuando un dato es correcto(√) o incorrecto(x)	*Parámetro nuevo*
		*Se añadió un * a cada campo que es requerido.*	*Parámetro nuevo*
	Cancelar: Parámetro utilizado para salir de la página e ingresar a una nueva.		*Eliminado*
		Estado de usuario: El estado del usuario puede modificarse a inactivo, en caso de ausencia temporal en el sistema y activo si todavía es parte de la institución.	*Ningún usuario es eliminado de la aplicación.*
Certificado	Disponibilidad de certificados	*Control del número de certificados activos del usuario.*	*Un usuario podrá disponer de un único certificado activo*

Categoría		*Validador de cada campo, que permita saber cuando un dato es correcto(√) o incorrecto(x)*	*Parámetro nuevo*
		*Se añadió un * a cada campo que es requerido.*	*Parámetro nuevo*
	Cancelar: Parámetro utilizado para salir de la página e ingresar a una nueva.		*Eliminado*
		Opción para elegir una plantilla y sea asignada a la categoría seleccionada.	*Parámetro nuevo*
Departamento		*Validador de cada campo, que permita saber cuando un dato es correcto(√) o incorrecto(x)*	*Parámetro nuevo*
		*Se añadió un * a cada campo que es requerido.*	*Parámetro nuevo*
	Cancelar: Parámetro utilizado para salir de la página e ingresar a una nueva.		*Eliminado*
Plantilla		*Validador de cada campo, que permita saber cuando un dato es correcto(√) o incorrecto(x)*	*Módulo nuevo*
Plantilla		*Se añadió un * a cada campo requerido*	*Módulo nuevo*
	Cancelar: Parámetro utilizado para salir de la página e ingresar a una nueva.	*Eliminado*	
		Elegir plantillas almacenadas en el sistema	
		Panel de ayuda para elegir tokens que permiten seleccionar encabezado y pie de página	
		Eliminar plantilla: Función que permite eliminar una plantilla que ha sido creada.	
Parámetro		*Validador de cada campo, que permita saber cuando un dato es correcto(√) o incorrecto(x)*	*Módulo nuevo*
		*Se añadió un * a los campos que son requeridos*	

Parámetro	**Cancelar:** Parámetro utilizado para salir de la página e ingresar a una nueva.	*Eliminado*	*Módulo nuevo*
		Descripción en cada parámetro que se puede editar	
Documento		*Validador de cada campo, que permita saber cuando un dato es correcto(√) o incorrecto(x)*	
		*Se añadió un * a cada campo que es requerido*	
	Cancelar: Parámetro utilizado para salir de la página e ingresar a una nueva.	*Eliminado*	
		Cambio de estado de un documento luego de ser leído.	*Parámetro nuevo*
		Bandeja de borradores: Documentos que son creados por el usuario y que más tarde pueden utilizarse.	*Parámetro nuevo*
		Bandeja de Eliminados: Documentos eliminados por el usuario.	*Parámetro nuevo*
		Asignador de plantilla en base a la categoría elegida por el usuario al momento de crear un documento.	*Parámetro nuevo*
		Opción de utilizar o no una plantilla	*Parámetro nuevo*
		Guardar Borrador: Parámetro que permite guardar un documento que se encuentra en edición.	*Parámetro nuevo*
		Reenviar: Parámetro que permite que un documento recibido pueda enviarse a uno o varios destinatarios. Esta opción se encuentra en la bandeja de entrada.	*Parámetro nuevo*

Documento		*Ruta del documento: Parámetro que permite verificar el recorrido que tuvo un documento antes de llegar a su destinatario final.*	*Parámetro nuevo*
Reporte		*Validador de fechas: La fecha inicial no puede ser mayor a la final y viceversa.*	*Módulo nuevo*
		Generación de reportes gráficos	*Los reportes se generarán tanto en forma escrita como en forma gráfica.*
		Generación de archivos log's	*Parámetro nuevo*
Respaldo		*Crear nuevo respaldo: Parámetro utilizado para crear un respaldo en forma manual*	*Módulo nuevo*
		Respaldo automático: Función que permite generar un respaldo en una hora establecida en el sistema.	
		Eliminar respaldo: Función que permite eliminar el respaldo generado.	
Interfaz	Menú : Usuarios, Categorías, Departamentos Parámetros	*Menú Administrar: Función para acceder a usuarios, categorías, departamentos, y parámetros.*	*Interfaz Menú principal*

Tabla 83. Control de Calidad

11. CONCLUSIONES

La gestión documental se ha convertido en una necesidad y en un problema para las organizaciones, debido a que deben garantizar el estado de conservación, tiempo, y búsqueda de documentos. La mayoría de las organizaciones necesitan acceder y consultar de forma frecuente la información archivada. En vista de ello y luego del análisis, diseño y desarrollo del Sistema de Gestión Documental para el Municipio de Calvas concluimos que:

1. La organización de la documentación en el Municipio de Calvas se encuentra estipulada en base a normas y reglamentos que rigen a la institución, para ello establecimos categorías que nos permitan identificar la clasificación de cada documento.
2. La generación de certificados internos en la institución permite que los usuarios puedan enviar o recibir información segura y auténtica a través de la red interna. Para lo cual el Municipio de Calvas por el momento actuara como entidad certificadora, a pesar de no ser reconocida legalmente como tal.
3. Las funciones hash son las encargadas de generar un resumen del contenido del mensaje que se enviará, para llevar a cabo este proceso se utilizó el algoritmo MD5, el cual permitió obtener una cadena de 32 bits en notación hexadecimal del mensaje original, el cual será comparado con el hash generado por el destinatario, y verificar así la autenticidad del documento que se recibió.
4. El aplicar claves privadas al contenido del mensaje permite garantizar seguridad y confidencialidad en la información que se envía entre una y varias oficinas. El algoritmo utilizado para la generación de claves y encriptación de mensajes fue el RSA.
5. La auditoría del sistema se basó principalmente en evidenciar los accesos y acciones en los diferentes módulos del sistema por parte de cada uno de los usuarios.
6. Se definió los roles de usuario y administrador para acceder a la aplicación, esto con la finalidad de evitar cambios o accesos no autorizados en la información.
7. La generación de reportes permite tener una mejor visualización de la forma en que los usuarios utilizaron el sistema. Los archivos log's por su parte permiten tener un mejor seguimiento de todo este proceso.

8. El sistema se encarga directamente de generar respaldos tanto automáticos como manuales; de la base de datos, archivos subidos e imágenes.

12. RECOMENDACIONES

En base a las conclusiones antes indicadas se recomienda lo siguiente:

1. Automatizar en lo posible todos los procesos documentales ya que su finalidad es el de convertirse en herramientas que garanticen el acceso a la información de manera rápida y oportuna.

2. Adaptar o crear una nueva versión de la aplicación en la que se permita utilizar tokens o dispositivos criptográficos otorgados por autoridades de certificación debidamente legalizadas como lo es el Banco Central del Ecuador.

3. Utilizar mecanismos como la encriptación en las aplicaciones que utilicen contraseñas o demás datos de carácter privado. Se puede recurrir tanto al uso de algoritmos de encriptación como de funciones hash.

4. Utilizar algoritmos de encriptación asimétrica para cifrar/ descifrar la información, debido a que es un tipo de algoritmo que garantiza mayor seguridad en la transferencia de datos al utilizar un par de claves únicas (privada y pública) para cada usuario.

5. Auditar cada una de las acciones que se dan en las aplicaciones, para mantener siempre activo el seguimiento de todo este proceso.

6. Definir roles y contraseñas para acceder a las aplicaciones con la finalidad de que la información administrada no sufra alteraciones.

7. Apoyar el seguimiento de las acciones que se dan en las aplicaciones a través de la generación de reportes gráficos y escritos, así como también generar archivos log's para garantizar los accesos ocurridos por cada usuario en el sistema.

8. Emigrar las bases de datos que se manejan en las aplicaciones a dispositivos seguros que eviten la pérdida de la misma, o en su defecto almacenar los respaldos que se generan en formatos comprimidos con la finalidad de optimizar espacio en el equipo servidor

13. BIBLIOGRAFÍA Y REFERENCIAS

- LLULL, Eduard. 2001 Criptografía - Firmas digitales [en linea] Disponible en [http://bulma.net/body.phtml?nIdNoticia=868] España [Consulta: 15 Enero 2010]
- Cámara de Gipuzcoa, 2005 Certificación Digital [en línea] Disponible en: [http://www.camaragipuzkoa.com/certificaciondigital/informacion_general/CAs.php] [Consulta: 10 de Enero del 2010].
- SAVOLAINEN, Martti, 2004 Métodos de Encriptación [en linea] Disponible en [http://www.cibernarium.tamk.fi/seguridad_2/salausmenetelmat.htm]Mexico [Consulta: 22 Enero 2010]
- LABORERO, Diego , 2008 Firma Digital [en linea] Disponible en [http://cxo-community.com.ar/index.php?option=com_content&task=view&id=1281&Itemid=1&utm_source=emBlue_Boletin$16&utm_medium=Oferta:617407]Sevilla [Consulta: 22 Enero 2010]
- VEGA Lebrún GUTIÉRREZ , Arvizu y GARCÍA Santillán**,** 2008 *Algoritmos para encriptación de datos*, Edición electrónica gratuita.[en linea] Disponible en [http: //www.eumed.net/libros/2008a/348/]Colombia[Consulta: 22 Enero 2010]
- Wikipedia, 2010 Flujo del Sistema de Gestión Documental [en línea] Disponible en [http://es.wikipedia.org/wiki/Gestión_documental] [Consulta: 10 de Enero del 2010]
- Wikipedia, 2010 MD5 [en línea] Disponible en [http://es.wikipedia.org/wiki/MD5] [Consulta: 10 de Enero del 2010]
- Wikipedia, 2010 Secure Hash Algorithm [en línea] Disponible en: [http://es.wikipedia.org/wiki/Secure_Hash_Algorithm] [Consulta: 10 de Enero del 2010]
- Wikipedia, 2010 Seguridad de la información [en línea] Disponible en [http://es.wikipedia.org/wiki/Seguridad_de_la_información] [Consulta: 15 de Enero del 2010]

- Wikipedia, 2010 JavaServer Faces [en línea] Disponible en: [http://es.wikipedia.org/wiki/JavaServer_Faces] [Consulta: 20 de Enero del 2010]

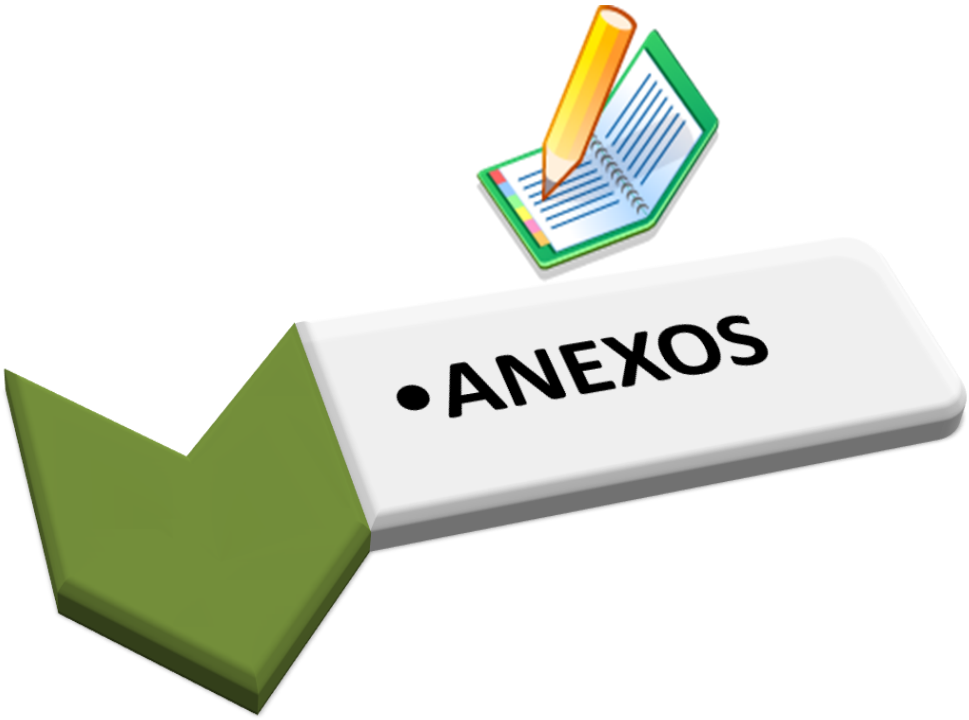
- RAMON, Santiago, 2005 Funciones Hash [en linea] Disponible en [http://foro.elhacker.net/criptografia/funciones_de_hash-t100025.0.html] Mèxico[Consulta: 30 Enero 2010]

- Sanromán, J, (2007) ¿Que es Jasper Reports? [en línea] Disponible en **[** http://www.jsanroman.net/2007/11/20/%C2%BFque-es-jasper-reports-2/] [Consulta: 20 de Enero del 2010]

- MACKAY, Patrick, 2004 Encriptación Asimétrica [en linea] Disponible en [http://msmvps.com/blogs/pmackay/archive/2004/11/27/easim1.aspx] Argentina[Consulta: 20 de Enero del 2010]

- NAVARRO , X, 2000 ¿Qué es un certificado digital? [en linea] Disponible en [http://www.poliedric.com/docs/certdigital.php]Barcelona [Consulta: 04 Febrero 2010]

- SANTOS, Sergio. Seguridad – Firma digital [en linea] Disponible en [http: //portalmundos.com/mundoinformatica/internet/firmadigital.html] España [Consulta: 15 Enero 2010]


•ANEXOS

14. ANEXOS

ANEXO 1:

GLOSARIO DE TÉRMINOS

A

Autenticación: Consiste en la verificación de la identidad de un usuario. En el caso de la firma digital, consiste en la firma del documento por parte del remitente antes de proceder al envío.

Adjunto: Archivo (texto, gráfico, etc.) vinculado a un correo electrónico o mensaje.

Administrador: Es la persona o programa encargado de gestionar, realizar el control, conceder permisos, etc. de todo un sistema informático o red de ordenadores.

Algoritmo criptográfico: Conjunto finito de operaciones matemáticas, reglas o pasos, que permiten obtener un texto cifrado a partir de un texto en claro.

Auditoría: Conjunto de técnicas y procedimientos sistemáticos, independientes y documentados para evaluar y controlar, un sistema informático y verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática.

Apache Tomcat: Es un servidor web con soporte de servlets y JSPs, desarrollado bajo el proyecto Jakarta en la Apache Software Foundation.

B

Base de datos: Es una colección estructurada de tablas que contienen datos.

Backup: Acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la pérdida de los originales.

Browser (navegador): (Explorer, Mozilla.) Consiste en un programa de aplicación con el que el usuario puede acceder a los documentos de la World Wide Web.

Bit (dígito binario): Es la unidad más pequeña de la información digital con la que trabajan los sistemas informáticos. Puede tener dos estados "0" o "1". La unión de 8 bits da lugar a un byte.

C

Categoría: Es un tipo de documento, que sirve para clasificar los mismos de una manera más ordenada.

Confidencialidad: Consiste en la utilización de técnicas de cifrado o encriptación que garanticen que sólo el usuario destinatario puede leer el mensaje.

Certificado Digital: Es el documento digitalmente emitido y firmado por una Entidad de Certificación, que identifica unívocamente a un suscriptor durante el período de vigencia de dicho certificado.

Clave criptográfica privada: Son valores numéricos o caracteres binarios que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos o de un documento digital.

Clave criptográfica pública: Son valores numéricos o caracteres binarios que son utilizados para verificar que una firma digital fue generada con la clave privada del suscriptor del certificado que ha emitido el mensaje de datos o el documento digital.

Criptografía: Es la rama de las matemáticas aplicadas a la ciencia informática que se ocupa de la transformación de documentos digitales o mensajes, de su representación original a una representación ininteligible e indescifrable que protege y preserva su contenido, y de la recuperación del documento o mensaje original a partir de ésta.

Cifrado asimétrico: Algoritmo de cifrado que necesita dos claves distintas. Cada usuario genera un par de claves usadas para el cifrado y el descifrado de mensajes, una de ellas la pone a disposición pública, clave pública y otra es la clave privada.

Cifrado simétrico Algoritmo de cifrado que requiere que ambas partes compartan una clave secreta; se usa la misma clave para cifrar y descifrar

Contraseña /Password: Clave para acceder a un determinado sistema.

Cliente: Un ordenador o un programa que accede a los servicios ofrecidos por otro ordenador o programa llamado servidor, al que está conectado en red.

D

DAO (Data Access Object**):** Es un componente de software que suministra una interfaz común entre la aplicación y uno o más dispositivos de almacenamiento de datos, tales como una Base de datos o un archivo

Departamento: Partes en las que se encuentra subdivido el Ilustre Municipio de Calvas, de acuerdo a las funciones que se deben llevar a cabo.

Descarga (Download): Proceso en el cual la información es transferida desde un servidor de información al propio ordenador personal.

Descifrar Proceso inverso al cifrado, es decir, obtener el mensaje en claro a partir del texto cifrado.

Destinatario: La persona designada por el iniciador para recibir el mensaje, pero que no está actuando a título de intermediario con respecto a ese mensaje.

E

Entidad de Certificación: Es aquella institución que está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.

Encriptación: El cifrado es el tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos.

F

Firma digital: Es la parte del certificado que permite al emisor garantizar su identidad en el envío de datos electrónicos. La firma digital se basa en la confianza que ofrece la infraestructura de clave pública y privada.

Funciones hash: Permiten obtener un resumen asociado a los datos generales y garantiza que no sean posibles dos mensajes diferentes con un "resumen" hash idéntico.

G

Gestión de Claves: Proceso para generar, transportar, almacenar y destruir claves de encriptación de modo seguro.

H

Hash: Un valor hash es un número generado a partir de una cadena de texto. El hash es sustancialmente más pequeño que el texto en sí, y es generado por una fórmula que sea poco probable que algún otro texto produzca el mismo valor.

HTML: (Hyper Text Markup Language) Es el lenguaje de marcado usado como el estándar para especificar el formato y delimitar el contenido que permite la visualización de páginas Web, desde un navegador.

HTTP (Hyper Text Transfer Protocol): Es un protocolo de comunicación que permite la visualización de páginas Web desde un navegador

HTTPS (Secure Hyper Text Transfer Protocol): El Protocolo Seguro de Transferencia de Hipertexto es utilizado para establecer conexiones del tipo HTTP pero de forma segura, utilizando TLS

I

Intranet: Red privada que utiliza el mismo tipo de software que Internet pero que es accesible solo para una comunidad de usuarios autorizados.

Integridad: Característica de la firma electrónica avanzada, que garantiza que la información contenida en el mensaje queda protegida y no puede ser manipulada o modificada durante el proceso.

Iniciar sesión: Identificarse y obtener acceso a un equipo mediante nombre de usuario y contraseña.

J

Java: Se refiere al lenguaje de programación Java, que fue diseñado para usar con la plataforma Java

Jasper Report: Es una librería para la generación de informes. Está escrita en java y es libre.

JFreeChart: Es una librería libre para la generación de todo tipo de graficas

JSF(Java Server Faces): Es un framework para construir interfaces de usuario en aplicaciones web.

JSP (Página de Servidor Java): Es un tipo especial de página HTML que contiene unos pequeños programas, llamados scripts que son ejecutados en el servidor antes de ser enviados al usuario para su visualización en forma de página HTML.

JDK (Java Development Kit): Es un compilador y conjunto de herramientas de desarrollo para la creación de programas independientes y applets java.

L

Log: Fichero de texto en el que queda recogida toda la actividad que tiene lugar en un determinado ordenador, permitiendo para ciertos programas que su propietario o administrador detecte e identifique, por medio de su dirección IP, al usuario correspondiente.

Login: Nombre que es requerido al acceder a un sistema informático y que identifica al usuario. También sirve para que el usuario se identifique ante su proveedor de acceso Internet o al revisar el correo.

M

Modelo Vista Controlador (MVC): Es un estilo de arquitectura de software que separa los datos de una aplicación, la interfaz de usuario, y la lógica de control en tres componentes distintos.

MD5: Algoritmo que permite obtener el hash de un documento, con salida de 128-bits

Mysql: Es un sistema de gestión de bases de datos relacional multihilo y multiusuario.

N

NetBeans: es una plataforma que permite que las aplicaciones sean desarrolladas a partir de un conjunto de componentes se software llamados módulos:

No repudio: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje, cuando realmente lo ha emitido, y que un receptor niegue su recepción, cuando realmente lo ha recibido.

Nodo: Un nodo es el punto de unión entre varias redes.

P

PKI – Infraestructura de Clave Pública: Sistema de certificados digitales, Autoridades Certificadores y otras entidades de registro que verifican y autentican la validez de cada una de las partes implicadas en una transacción vía Internet.

Privacidad Derecho de los individuos a controlar e influir en la recogida y almacenamiento de datos relativos a ellos mismos, así como por quien y a quien pueden ser dados a conocer estos datos.

Plantilla: Es un esquema de documento que sirve para dar formato al mismo

R

Revocación: Anulación definitiva de un certificado digital, o bien, a petición del suscriptor, o bien, por propia iniciativa de la autoridad de certificación en caso de duda de la seguridad de las claves.

Repositorio: Es un sistema de información para el almacenamiento y recuperación de certificados u otro tipo de información relevante para la expedición y validación de los mismos.

Reportes: Es una descripción escrita y grafica de las acciones efectuadas en el sistema durante un periodo de tiempo.

RSA: Sistema criptográfico de clave pública, desarrollado en 1977. Es válido tanto para cifrar como para firmar digitalmente.

S

Servidor: Equipo que controla el acceso de los usuarios a una red y les da servicio e información. Sistema informático (ordenador) que presta ciertos servicios y recursos (de comunicación, aplicaciones, ficheros, etc.) a otros ordenadores (denominados clientes), los cuales están conectados en red a él.

Signatario: La persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

T

Titular: Ciudadano para el que se expide un certificado de identidad pública.

U

Upload: Subir un fichero a un servidor de Internet.

Usuario: Es la persona que, sin ser suscriptor y sin contratar los servicios de emisión de certificados de una Entidad de Certificación, puede, sin embargo, verificar la integridad y autenticidad de un documento digital o de un mensaje de datos, con base en un certificado del suscriptor originador del mensaje.

ANEXO 2:

TABLAS CONTENIDAS EN LA BASE DE DATOS

auditoria

Nombre	Tipo	N..	P..	Extras
Índice principal	idauditoria			unique
FKB8A64966905AFF7	idusuario			
idauditoria	bigint(20)	No		auto_increment
idusuario	bigint(20)	Sí		
aud_modulo	varchar(80)	No		
aud_accion	varchar(80)	No		
aud_descripcion	varchar(150)	No		
aud_fecha	datetime	Sí		
FKB8A64966905AFF7	idusuario -> usuario.idusuario			

borrador

Nombre	Tipo	N..	P..	Extras
Índice principal	idborrador			unique
FK7D036A136905AFF7	idusuario			
FK7D036A136BB99141	idcategoria			
idborrador	bigint(20)	No		auto_increment
idusuario	bigint(20)	Sí		
idcategoria	bigint(20)	Sí		
bor_fecha	datetime	Sí		
bor_titulo	varchar(200)	Sí		
bor_archivo	varchar(200)	Sí		
bor_tipo_archivo	varchar(200)	Sí		
bor_mensaje	text	Sí		
bor_comentario	text	Sí		
FK7D036A136905AFF7	idusuario -> usuario.idusuario			
FK7D036A136BB99141	idcategoria -> categoria.idcategoria			

categoría

Nombre	Tipo	N..	Extras
Índice principal	idcategoria		unique
cat_nombre	cat_nombre		unique
FK5D54E133755989F3	cat_plantilla		
idcategoria	bigint(20)	N..	auto_increm...
cat_plantilla	bigint(20)	Sí	
cat_nombre	varchar(45)	N..	
cat_referencia	varchar(8)	N..	
cat_fecha_creacion	datetime	N..	
FK5D54E133755989F3	cat_plantilla -> plantilla.idplantilla		

certificado

Nombre	Tipo	N..	P..	Extras
Índice principal	idcertificado			unique
FK745F3FB16905AFF7	idusuario			
idcertificado	bigint(20)	N..		auto_increm...
idusuario	bigint(20)	Sí		
cer_serie	varchar(80)	Sí		
cer_version	varchar(45)	Sí		
cer_algoritmo	varchar(45)	Sí		
cer_emisor	varchar(60)	Sí		
cer_motivo_baja	varchar(100)	Sí		
cer_fecha_creacion	datetime	N..		
cer_fecha_expiracion	datetime	N..		
cer_estado	bit(1)	Sí		
cer_sn	text	N..		
cer_se	text	N..		
cer_sd	text	N..		
cer_sp	text	N..		
cer_sq	text	N..		
cer_long_claro	int(11)	N..		
cer_long_cifrado	int(11)	N..		
FK745F3FB16905AFF7	idusuario -> usuario.idusuario			

departamento

Nombre	Tipo	N..	P..	Extras
Índice principal	iddepartamento			unique
dep_nombre	dep_nombre			unique
iddepartamento	bigint(20)	N..		auto_increm...
dep_nombre	varchar(45)	N..		
dep_referencia	varchar(5)	N..		
dep_descripcion	varchar(100)	N..		

documento

Nombre	Tipo	N..	P..	Extras
Índice principal	iddocumento			unique
FK383D52B46905AFF7	idusuario			
FK383D52B46BB99141	idcategoria			
FK383D52B49516037D	idcertificado			
FK383D52B47DAAA489	doc_padre			
iddocumento	bigint(20)	N..		auto_increment
doc_padre	bigint(20)	Sí		
idcategoria	bigint(20)	Sí		
idcertificado	bigint(20)	Sí		
idusuario	bigint(20)	Sí		
doc_fecha_creacion	datetime	Sí		
doc_comentario	text	Sí		
doc_titulo	varchar(200)	Sí		
doc_tipo_seguridad	varchar(45)	Sí		
doc_nombre_archivo	varchar(200)	Sí		
doc_tipo_archivo	varchar(200)	Sí		
FK383D52B46905AFF7	idusuario -> usuario.idusuario			
FK383D52B46BB99141	idcategoria -> categoria.idcategoria			
FK383D52B47DAAA489	doc_padre -> iddocumento			
FK383D52B49516037D	idcertificado -> certificado.idcertificado			

documento_usuario

Nombre	Tipo	N..	P..	Extras
Índice principal	iddocus			unique
FK5B8DF8A38D46A90D	dus_padre			
FK5B8DF8A36905AFF7	idusuario			
FK5B8DF8A3218A7443	iddocumento			
iddocus	bigint(20)	N..		auto_increment
dus_padre	bigint(20)	Sí		
dus_numero	bigint(20)	Sí	0	
iddocumento	bigint(20)	N..		
idusuario	bigint(20)	N..		
dus_estado	varchar(20)	N..		
dus_hash	text	Sí		
dus_encabezado	text	Sí		
dus_pie	text	Sí		
dus_mensaje_encriptado	longblob	Sí		
FK5B8DF8A3218A7443	iddocumento -> documento.iddocumento			
FK5B8DF8A36905AFF7	idusuario -> usuario.idusuario			
FK5B8DF8A38D46A90D	dus_padre -> iddocus			

parametro

Nombre	Tipo	N.	P..	Extras
Índice principal	idparametro			unique
par_codigo	par_codigo			unique
idparametro	bigint(20)	N.		auto_increment
par_codigo	varchar(80)	N.		
par_valor	text	N.		
par_descripcion	text	N.		
par_tipo	varchar(20)	Sí		

plantilla

Nombre	Tipo	N.	P..	Extras
Índice principal	idplantilla			unique
pla_nombre	pla_nombre			unique
idplantilla	bigint(20)	N.		auto_increment
pla_nombre	varchar(80)	N.		
pla_plantilla_encabezado	text	Sí		
pla_plantilla_pie	text	Sí		

usuario

Nombre	Tipo	N.	P..	Extras
Índice principal	idusuario			unique
usu_login	usu_login			unique
FKF814F32E4693574D	iddepartamento			
idusuario	bigint(20)	N.		auto_increment
estado	bit(1)	Sí		
iddepartamento	bigint(20)	Sí		
usu_login	varchar(30)	N.		
usu_clave	varchar(250)	N.		
usu_indicio_clave	varchar(60)	Sí		
usu_trato	varchar(45)	Sí		
usu_rol	varchar(15)	Sí		
usu_nombres	varchar(30)	Sí		
usu_apellidos	varchar(30)	Sí		
usu_cedula	varchar(10)	N.		
usu_fecha_registro	datetime	Sí		
usu_fecha_nacimiento	datetime	Sí		
usu_direccion	text	Sí		
usu_email	varchar(80)	Sí		
usu_telefono_domicilio	varchar(15)	Sí		
usu_telefono_trabajo	varchar(15)	Sí		
usu_telefono_movil	varchar(15)	Sí		
usu_sexo	varchar(1)	Sí		
usu_cargo	varchar(45)	Sí		
usu_lugar	varchar(45)	Sí		
FKF814F32E4693574D	iddepartamento -> departamento.iddepartamento			

ANEXO 3:

MODELO DE ENTREVISTA APLICADA AL PERSONAL DEL MUNICIPIO DE CALVAS

Como Egresados de la carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, solicitamos a usted de la manera más comedida se digne en responder el siguiente cuestionario, con la finalidad de obtener información relacionada con el proceso de gestión documental que actualmente se lleva a cabo en la institución.

1. ¿El proceso de gestión documental actualmente se lleva a cabo de forma?
   Manual ( ) Automática ( )
2. Existen inconvenientes al momento de tramitar algún tipo de documento ¿Cuáles son estos inconvenientes?
   ……
3. ¿Qué tipo de documentación se tramita dentro de la institución?
   ……
4. ¿Cada documento tiene algún identificativo en especial?
   Si ( ) No ( )
   Cuál……
5. ¿Cuál es la clasificación que se lleva a cabo actualmente en la documentación que se tramita?
   ……
6. ¿Qué tipo de documento es el que mayor demanda tiene para ser tramitado?
   ……
7. Describa el proceso que se debe seguir para tramitar algún tipo de documento
   ……

8. ¿Cuál es el tiempo requerido para tramitar un documento y de que factores depende?

……
.

9. ¿Los documentos que se tramitan en la institución suelen sufrir algún tipo de alteraciones, qué tipo de alteraciones?

Si ( ) No ( )

……

10. ¿Cuándo requieren documentos de fechas anteriores de que manera lo obtienen?

……
……

11. ¿La documentación tramitada de qué manera se almacena?

……
……

12. ¿Cuáles son los departamentos que conforman el Municipio de Calvas?

……
……

13. ¿Cuándo llega algún documento porque departamento es receptado?

……

14. ¿La mayor parte de documentos recibidos hacia que departamentos son enviados?

……

15. ¿Todos los departamentos tienen acceso a la red local de la institución?

Si ( ) No ( )

16. ¿Actualmente cuentan con servicio de mensajería entre todos los departamentos?

Si ( ) No ( )

GRACIAS POR SU COLABORACIÓN

ANEXO 4:

MODELO DE ENCUESTAS APLICADAS PARA LOS ADMINISTRADORES Y USUARIOS DEL SISTEMA

UNIVERSIDAD NACIONAL DE LOJA

ENCUESTA PARA EL ADMINISTRADOR

Como Egresados de la carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, solicitamos a usted de la manera más comedida se digne en responder la siguiente encuesta, con la finalidad de tener información relacionada con el funcionamiento y validación del "Sistema de Gestión Documental en la Ilustre Municipalidad del cantón Calvas"

1. ¿El acceso al sistema en cuanto a rapidez es?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

2. ¿El acceso al sistema en cuanto a seguridad es?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

3. ¿Qué tan amigable es la interfaz del sistema?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

4. ¿Su criterio en cuanto a la información de ayuda que presenta la aplicación durante su manipulación es?
   Excelente ( )
   Muy Bueno ( )

Bueno ( )
Regular ( )

5. ¿Cuál es su calificación con respecto al ingreso de datos en la aplicación?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

6. ¿Cuál es su calificación con respecto a la validación de datos en al aplicación?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

7. ¿Cuál es su opinión con respecto a los módulos con los que cuenta la aplicación actualmente?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

8. ¿Cuál es su criterio con respecto a las funcionalidades con las que cada módulo cuenta?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

9. ¿Qué calificación otorgaría a la búsqueda y organización de información a través del menú “Mis Documentos”?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

10. ¿Considera que el envió de mensajes en cuanto a rapidez es?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

11. ¿Considera que la recepción de mensajes en cuanto a rapidez es?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

12. ¿Cuál es su calificación con respecto al proceso para almacenamiento y recuperación de información?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

13. ¿Cuál es su criterio con respecto a la utilización de certificados digitales generados internamente para el envió y recepción de información?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

14. ¿Según su criterio cree usted que el proceso de seguimiento o ruta de un documento para tener un mejor conocimiento sobre la tramitación de información es?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

15. ¿Cuál es su criterio con respecto al uso de plantillas durante la creación de documentos?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

16. ¿Según su criterio el listado y generación de reportes existentes en el sistema para dar seguimiento a la aplicación es?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

17. ¿Según su criterio la parametrización de la información en el sistema es?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

18. ¿Según su criterio el proceso para la ejecución de respaldos automáticos y manuales es?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

19. ¿Cuál es su criterio con respecto a las referencias o sintaxis utilizadas para identificar a cada categoría, departamento o documento?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

GRACIAS POR SU COLABORACIÓN

UNIVERSIDAD NACIONAL DE LOJA

ENCUESTA PARA LOS USUARIOS

Como Egresados de la carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, solicitamos a usted de la manera más comedida se digne en responder la siguiente encuesta, con la finalidad de tener información relacionada con el funcionamiento y validación del "Sistema Automatizado para la Gestión Documental en la Ilustre Municipalidad del cantón Calvas"

1. ¿Cuando usted ingresa al sistema, considera que su rapidez es?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

2. ¿Cuál es su opinión con respecto al ambiente de trabajo en la aplicación?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

3. ¿Considera usted que la combinación de colores utilizados en la aplicación?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

4. ¿Considera usted que el tamaño y tipo de letras utilizadas en la aplicación es?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

5. ¿Considera usted que la distribución de tablas o representación de resultados es?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

6. ¿Cuál es su criterio referente a las pautas que el sistema le ofrece para que pueda utilizarlo?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

7. ¿Considera usted que las imágenes que el sistema incluye sobre el cantón Calvas es?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

8. ¿Cree usted que la información relacionada con el Municipio de Calvas es?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

9. ¿Cuándo usted busca información/documentos considera que el resultado es?
   Excelente ( )
   Muy Bueno ( )
   Bueno ( )
   Regular ( )

10. ¿Considera usted que la organización de sus documentos es?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

11. ¿Cómo considera usted al proceso de creación de documentos?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )

Regular ( )

12. ¿Cuándo usted desea enviar un documento, cuál es su criterio con respecto a su velocidad?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

13. ¿Considera usted que cuándo guarda o lee información en el sistema, este proceso es?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

14. Un certificado digital permite que la información que usted envía no sea conocida por el resto de personas, solamente puede leerla su destinatario, para ello se utiliza claves que permiten que el contenido de la información se transforme en un nuevo texto difícil de leer. Por lo tanto ¿Considera usted que el uso de certificados digitales para el envió y recepción de documentos para asegurar seguridad en la información es?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

15. ¿Según su criterio cree usted que el dar seguimiento a un documento para tener un mejor conocimiento sobre su tramitación es?
    Excelente ( )
    Muy Bueno ( )
    Bueno ( )
    Regular ( )

GRACIAS POR SU COLABORACIÓN

ANEXO 5

CERTIFICACIÓN DE HABER REALIZADO PRUEBAS AL SISTEMA

GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN CALVAS
SISTEMAS
CARIAMANGA-LOJA-ECUADOR

A petición de la parte interesada

CERTIFICO

Que el Sr. Franklin Freddy Andrade Alverca y la Srta. Patricia Elizabeth Chamba Briceño, realizaron las pruebas y validación de su proyecto de tesis denominado:

"DISEÑO Y CONSTRUCCIÓN DE UN SISTEMA AUTOMATIZADO PARA LA GESTIÓN DE DOCUMENTOS EN LA ILUSTRE MUNICIPALIDAD DEL CANTÓN CALVAS"

Previa autorización del Sr. Alcalde del Cantón, logrando las metas y objetivos que persigue este proyecto de tesis, y sin beneficio alguno de lucro.

Es todo cuanto puedo certificar al respecto en honor a la verdad, facultándoles a los interesados hacer uso en lo que a bien tuviere conveniente

Cariamanga, 16 de Junio del 2010

Atentamente,

…….
Ing. Darwin Jiménez Torres
ANALISTA DE SISTEMAS INFORMÁTICOS

ANEXO 6:

TABULACIÓN DE ENCUESTAS ADMINISTRADOR Y USUARIOS DEL SISTEMA

Análisis y discusión de resultados de las encuestas aplicadas a los administradores

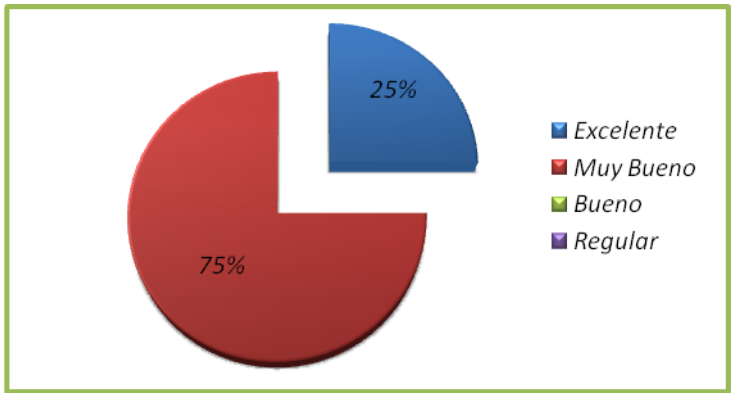
1. ¿El acceso al sistema en cuanto a rapidez es?

Tabla Nº 1

Variable	f	%
Excelente	1	25
Muy Bueno	3	75
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 1



Interpretación de resultados

De la información recolectada de 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del total de la población encuestada, se concluye que el 25% calificó el acceso al sistema en cuanto a rapidez como “Excelente”, mientras que el 75% como “Muy Bueno”

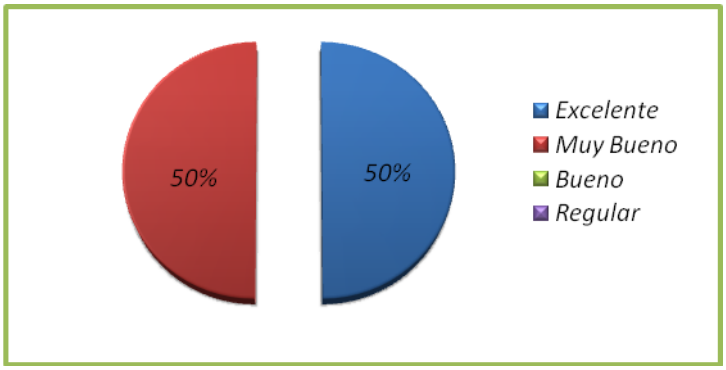
2. ¿El acceso al sistema en cuanto a seguridad es?

Tabla Nº 2

Variable	f	%
Excelente	2	50
Muy Bueno	2	50
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 2



Interpretación de resultados

En base a la información recolectada de 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del de dicha población encuestada, se concluye que el 50% califica el acceso al sistema en cuanto a seguridad como "Excelente", mientras que el otro 50% restante como "Muy Bueno"

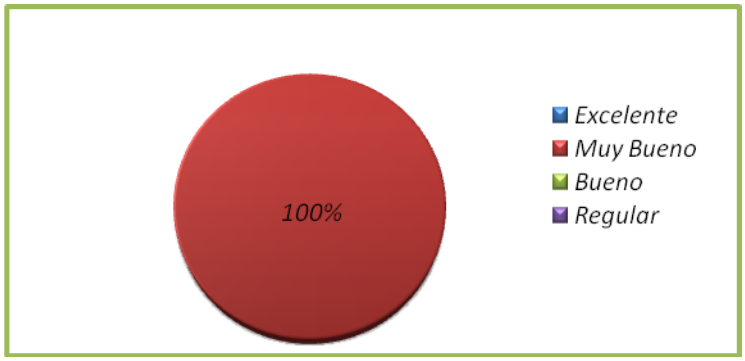
3. ¿Qué tan amigable es la interfaz del sistema?

Tabla Nº 3

Variable	f	%
Excelente	0	0
Muy Bueno	4	100
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 3



Interpretación de resultados

Mediante la encuesta aplicada a 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del total de la población, se concluye que la totalidad (100%) de los encuestados, califica como "Muy Bueno" a la interfaz utilizada en el sistema.

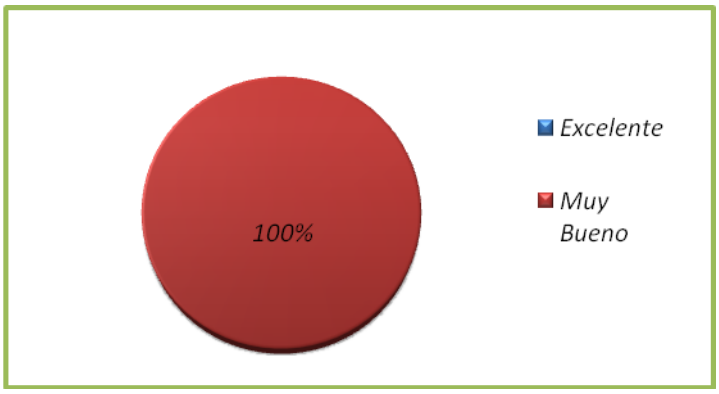
4. ¿Su criterio en cuanto a la información de ayuda que presenta la aplicación durante su manipulación es?

Tabla Nº 4

Variable	f	%
Excelente	0	0
Muy Bueno	4	100
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 4



Interpretación de resultados

De la información obtenida de 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del total de la población encuestada, se concluye que el 100% calificó que la información de ayuda que se encuentra en el sistema es "Muy Bueno"

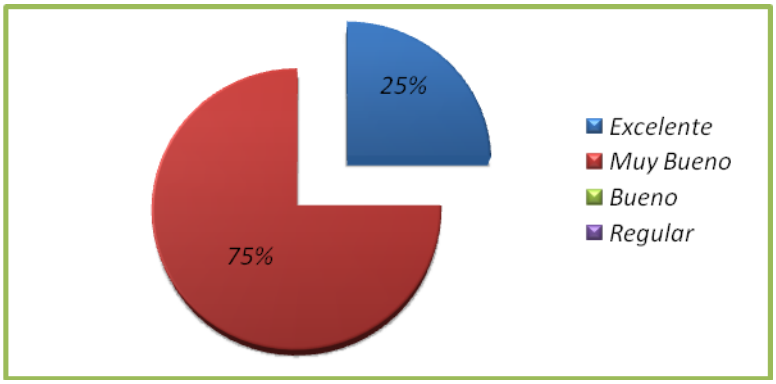
5. ¿Cuál es su calificación con respecto al ingreso de datos en la aplicación?

Tabla Nº 5

Variable	f	%
Excelente	1	25
Muy Bueno	3	75
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 5



Interpretación de resultados

En base a la información recolectada de 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del de dicha población encuestada, se concluye que el 25% calificó al ingreso de datos en el sistema como “Excelente”, mientras que el otro 75% restante como “Muy Bueno”

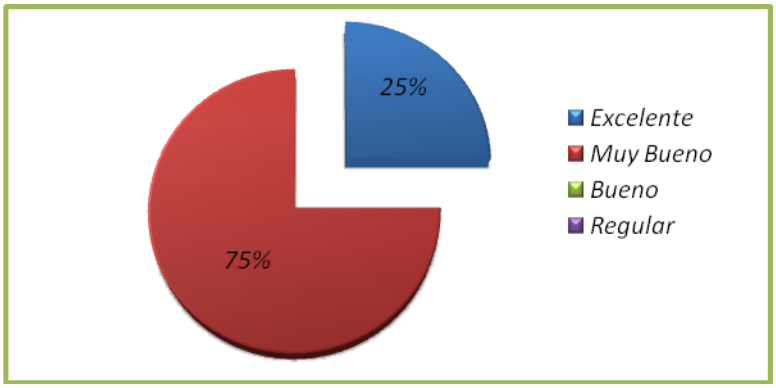
6. ¿Cuál es su calificación con respecto a la validación de datos en la aplicación?

Tabla Nº 6

Variable	f	%
Excelente	1	25
Muy Bueno	3	75
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 6



Interpretación de resultados

Mediante la encuesta aplicada a 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del total de la población, se concluye que el 25% de los encuestados, calificaron al proceso de validación de datos en el sistema como "Excelente", mientras que el 75% como "Muy Bueno".

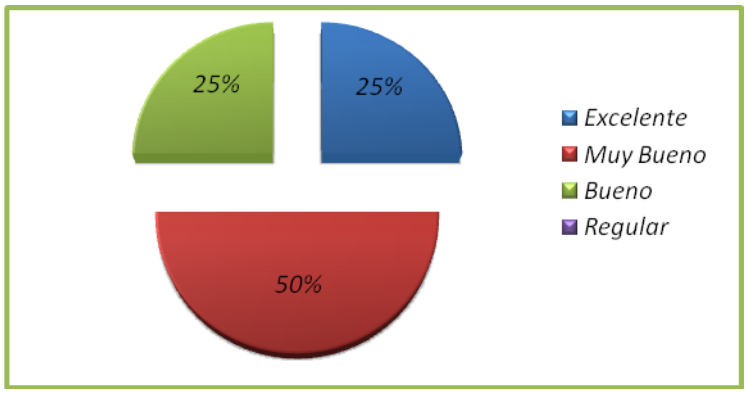
7. ¿Cuál es su opinión con respecto a los módulos con los que cuenta la aplicación actualmente?

Tabla Nº 7

Variable	f	%
Excelente	1	25
Muy Bueno	2	50
Bueno	1	25
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 7



Interpretación de resultados

De la información recolectada de 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del total de la población encuestada, se concluye que el 25% calificó como "Excelente" a la estructuración de módulos con que actualmente cuenta la aplicación, mientras que el 50% sostiene que "Muy Bueno" el 25% restante por su parte dio una calificación de "Bueno"

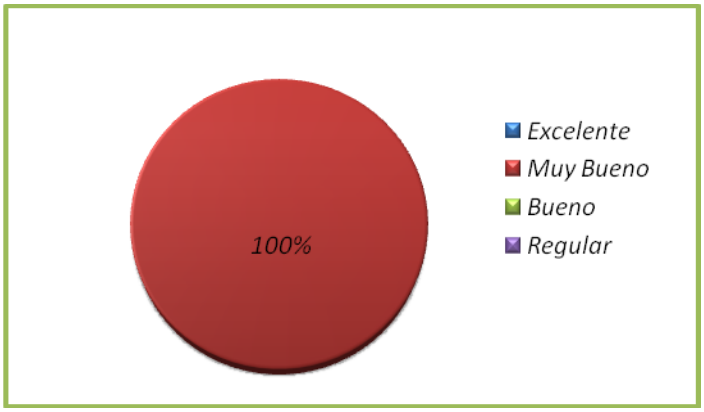
8. ¿Cuál es su criterio con respecto a las funcionalidades con las que cada módulo cuenta?

Tabla Nº 8

Variable	f	%
Excelente	0	0
Muy Bueno	4	100
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 8



Interpretación de resultados

En base a la información recolectada de 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% de dicha población encuestada, se concluye que el 100% calificó a las funcionalidades con que las que cuenta cada modulo del sistema como "Muy Bueno"

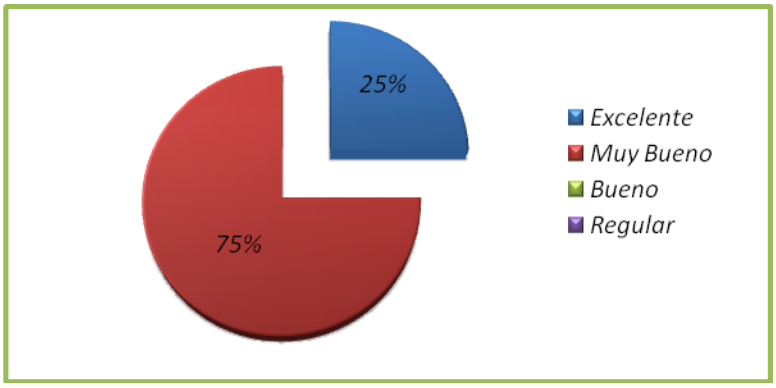
9. ¿Qué calificación otorgaría a la búsqueda y organización de información a través del menú "Mis Documentos"?

Tabla Nº 9

Variable	f	%
Excelente	1	25
Muy Bueno	3	75
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 9



Interpretación de resultados

De la información recolectada de 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del total de la población encuestada, se concluye que el 25% calificó al proceso de búsqueda y organización de la información mediante la opción de "Mis Documentos" como "Excelente", por su parte el 75% restante como "Muy Bueno"

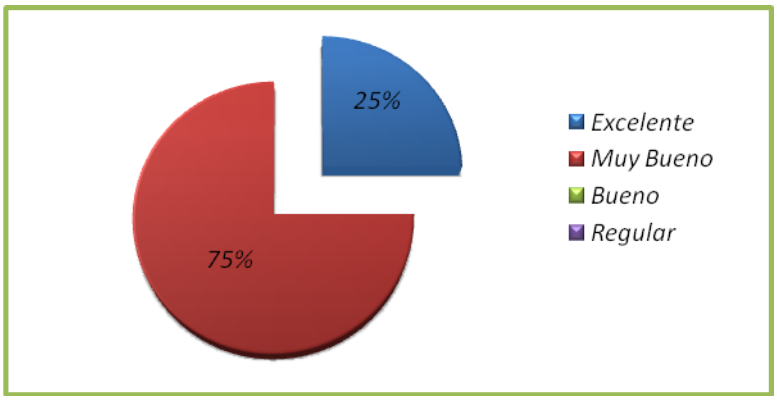
10. ¿Considera que el envió de mensajes en cuanto a rapidez es?

Tabla Nº 10

Variable	f	%
Excelente	1	25
Muy Bueno	3	75
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 10



Interpretación de resultados

Mediante la encuesta aplicada a 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del total de la población, se concluye que el 25% de los encuestados, calificaron al proceso de envío de mensajes en cuanto a rapidez como "Excelente" en tanto que el 75% indicaron que su criterio es de "Muy Bueno"

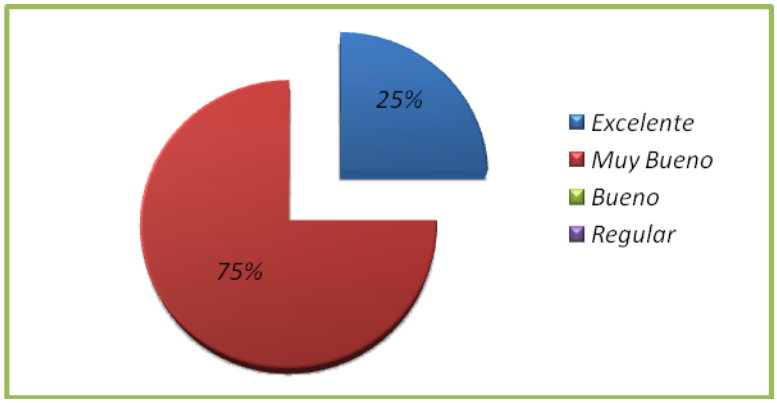
11. ¿Considera que la recepción de mensajes en cuanto a rapidez es?

Tabla Nº 11

Variable	f	%
Excelente	1	25
Muy Bueno	3	75
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 11



Interpretación de resultados

De la información recolectada de 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del total de la población encuestada, se concluye que el 25% de los encuestados, calificaron al proceso de recepción de mensajes en cuanto a rapidez como "Excelente" por su parte el 75% restante opinaron que es "Muy Bueno"

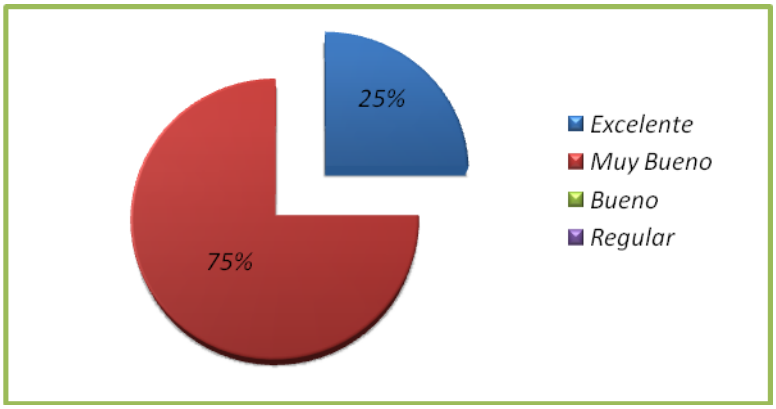
12. ¿Cuál es su calificación con respecto al proceso para almacenamiento y recuperación de información?

Tabla Nº 12

Variable	f	%
Excelente	1	25
Muy Bueno	3	75
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 12



Interpretación de resultados

En base a la información recolectada de 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% de dicha población encuestada, se concluye que el 25% calificaron como "Excelente" al proceso de almacenamiento y recuperación de la información en el sistema, el 75% restante por su parte indicaron que es "Muy Bueno"

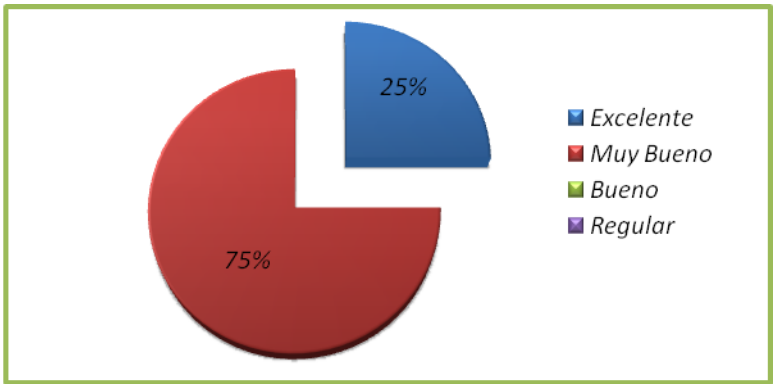
13. ¿Cuál es su criterio con respecto a la utilización de certificados digitales generados internamente para el envió y recepción de información?

Tabla Nº 13

Variable	f	%
Excelente	1	25
Muy Bueno	3	75
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 13



Interpretación de resultados

Mediante la encuesta aplicada a 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del total de la población, se concluye que el 25% de los encuestados, calificaron como "Excelente" a la utilización de certificados digitales generados internamente en el sistema para el envió y recepción de información, en tanto que el 75% restante supo manifestar que la utilización de certificados digitales en el sistema es "Muy Bueno"

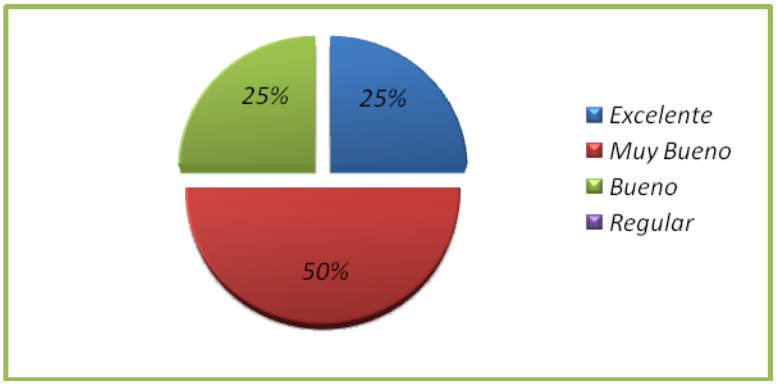
14. ¿Según su criterio cree usted que el proceso de seguimiento o ruta de un documento para tener un mejor conocimiento sobre la tramitación de información es?

Tabla Nº 14

Variable	f	%
Excelente	1	25
Muy Bueno	2	50
Bueno	1	25
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 14



Interpretación de resultados

De la información recolectada de 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del total de la población encuestada, se concluye que el 25% calificó al proceso de seguimiento o ruta de un documento para tener un mejor conocimiento sobre su tramitación como "Excelente", por su parte el 50% indicó que es "Muy Bueno" mientras que el 25% restante considera que el seguimiento de la información en tramitación es "Bueno"

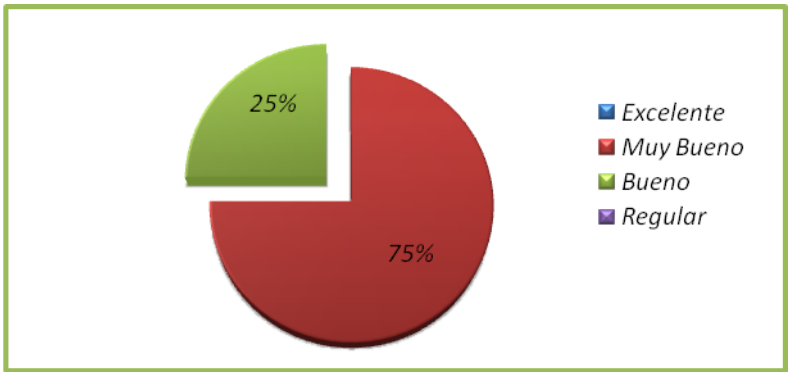
15. ¿Cuál es su criterio con respecto al uso de plantillas durante la creación de documentos?

Tabla Nº 15

Variable	f	%
Excelente	0	0
Muy Bueno	3	75
Bueno	1	25
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 15



Interpretación de resultados

En base a la información recolectada de 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del de dicha población encuestada, se concluye que el 75% de calificaron como "Muy Bueno" al proceso de generación de plantillas para la creación de documentos, el 25% restante indicaron que este proceso es "Bueno".

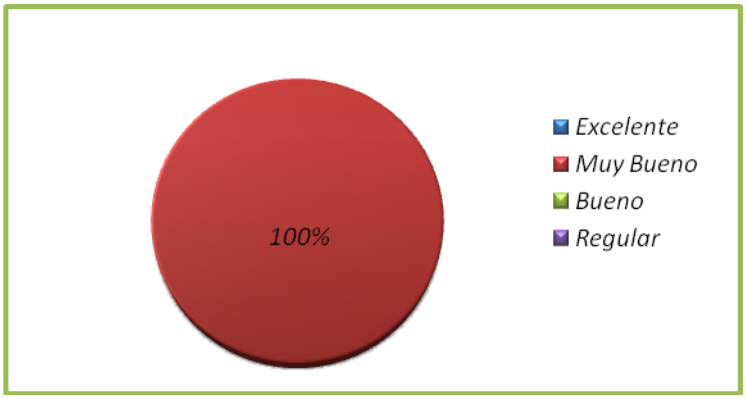
16. ¿Según su criterio el listado y generación de reportes existentes en el sistema para dar seguimiento a la aplicación es?

Tabla Nº 16

Variable	f	%
Excelente	0	0
Muy Bueno	4	100
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 16



Interpretación de resultados

Mediante la encuesta aplicada a 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del total de la población, se concluye que el 100% de los encuestados calificaron que la generación de reportes en el sistema para dar seguimiento a la aplicación es "Muy Bueno"

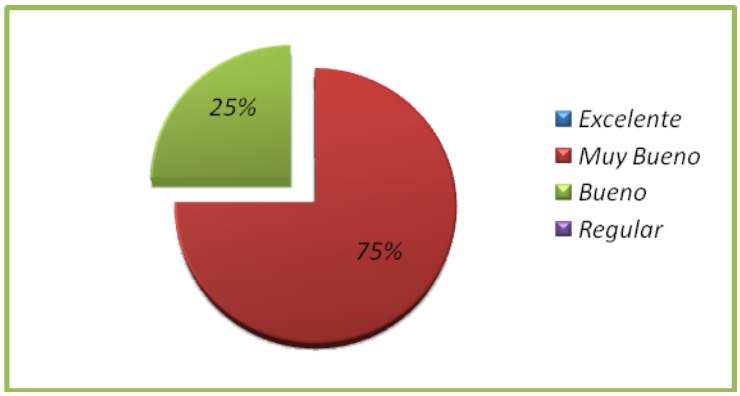
17. ¿Según su criterio la parametrización de la información en el sistema es?

Tabla Nº 17

Variable	f	%
Excelente	0	0
Muy Bueno	3	75
Bueno	1	25
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 17



Interpretación de resultados

De la información recolectada de 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del total de la población encuestada, se concluye que el 75% calificó al proceso de parametrización de la información en el sistema como "Muy Bueno", por su parte el 25% restante indicó que dicho proceso es "Bueno.

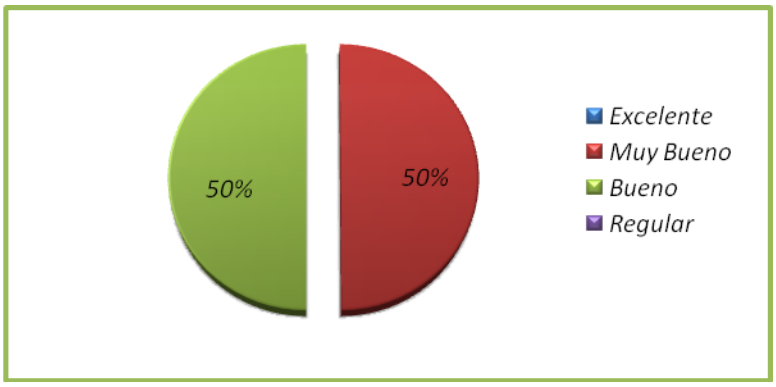
18. ¿Según su criterio el proceso para la ejecución de respaldos automáticos y manuales es?

Tabla Nº 18

Variable	f	%
Excelente	0	0
Muy Bueno	2	50
Bueno	2	50
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 18



Interpretación de resultados

En base a la información recolectada de 4 administradores/as del departamento del GADCC que representan el 100% de dicha población encuestada, se concluye que el 50% calificó al proceso para la ejecución de respaldos automáticos y manuales como "Muy Bueno", mientras que el otro 50% restante manifestó que es "Bueno"

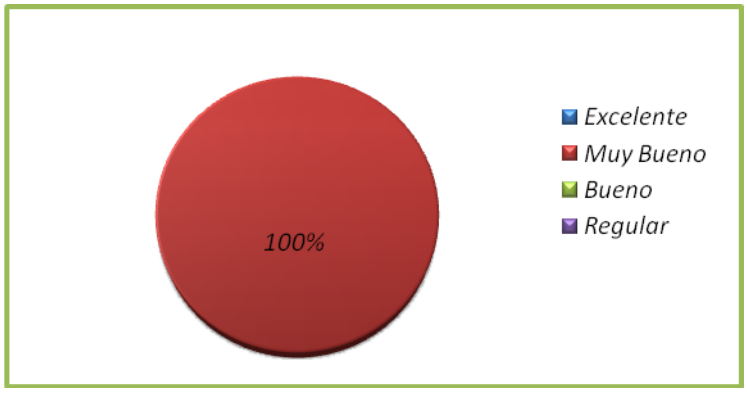
19. ¿Cuál es su criterio con respecto a las referencias o sintaxis utilizadas para identificar a cada categoría, departamento o documento?

Tabla Nº 19

Variable	f	%
Excelente	0	0
Muy Bueno	4	100
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Administradores del departamento de Sistemas del GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 19



Interpretación de resultados

Mediante la encuesta aplicada a 4 administradores/as del departamento de Sistemas del GADCC que representan el 100% del total de la población, se concluye la totalidad (100%) de los encuestados, calificó como "Muy Bueno" a las referencias o sintaxis utilizadas en el sistema para identificar a cada categoría, departamento o documento.

Análisis y discusión de resultados de las encuestas aplicadas a los usuarios

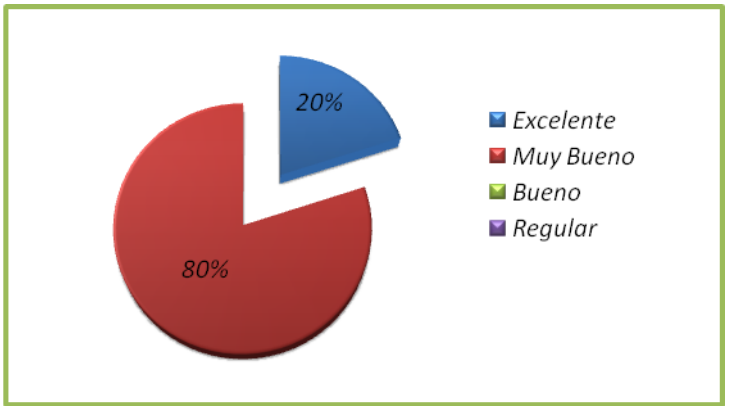
20. ¿Cuándo usted ingresa al sistema, considera que su rapidez es?

Tabla Nº 20

Variable	f	%
Excelente	2	20
Muy Bueno	8	80
Bueno	0	0
Regular	0	0
TOTAL	**10**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 20



Interpretación de resultados

De la información recolectada de 10 usuarios/as de la aplicación en el GADCC que representan el 100% del total de la población encuestada se concluye que, el 20% calificó al acceso al sistema en cuanto a rapidez como "Excelente", mientras que el 80% como "Muy Bueno"

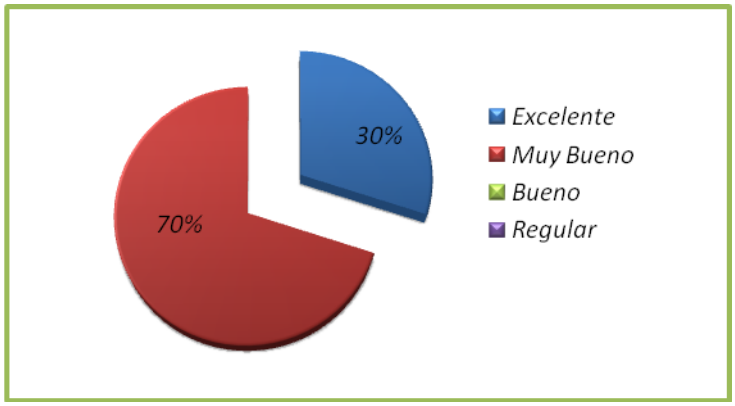
21. ¿Cuál es su opinión con respecto al ambiente de trabajo en la aplicación?

Tabla Nº 21

Variable	f	%
Excelente	3	30
Muy Bueno	7	70
Bueno	0	0
Regular	0	0
TOTAL	**10**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 21



Interpretación de resultados

En base a la información recolectada de 10 usuarios/as de la aplicación en el GADCC que representan el 100% del dicha de la población encuestada, y según como se observa en el gráfico, se concluye que, el 30% calificó al ambiente de trabajo e interfaz amigable en la aplicación como "Excelente", mientras que el otro 70% le dio una calificación de "Muy Bueno"

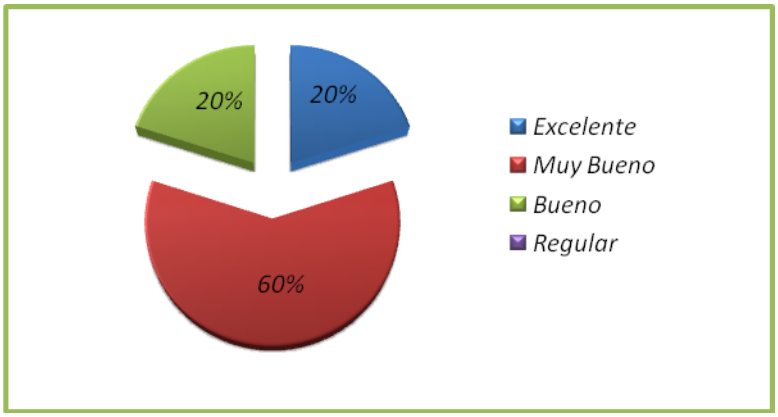
22. ¿Considera usted que la combinación de colores utilizados en la aplicación?

Tabla Nº 22

Variable	f	%
Excelente	2	20
Muy Bueno	6	60
Bueno	2	20
Regular	0	0
TOTAL	**10**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 22



Interpretación de resultados

Mediante la encuesta aplicada a 10 usuarios/as de la aplicación en el GADCC que representan el 100% del dicha de la población encuestada, se conoció que el 20% de la población, considera que la combinación de colores usados en la aplicación es "Excelente", un 60% calificó que la combinación de colores es "Muy Bueno" mientras que el 20% le dio una calificación de "Bueno".

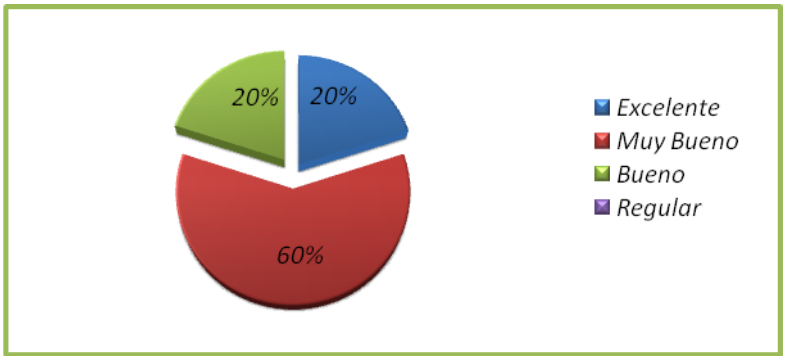
23. ¿Considera usted que el tamaño y tipo de letras utilizadas en la aplicación es?

Tabla Nº 23

Variable	f	%
Excelente	2	20
Muy Bueno	6	60
Bueno	2	20
Regular	0	0
TOTAL	**10**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 23



Interpretación de resultados

De la información obtenida de 10 usuarios/as de la aplicación en el GADCC que representan el 100% del total de la población encuestada, se concluye que, el 20% calificó al tamaño y tipo de letra utilizados en la aplicación como "Excelente" en tanto que el 60% considera que es "Muy Bueno", mientras que el 20% restante califica que el tipo y tamaño de letra usados en la aplicación es "Bueno"

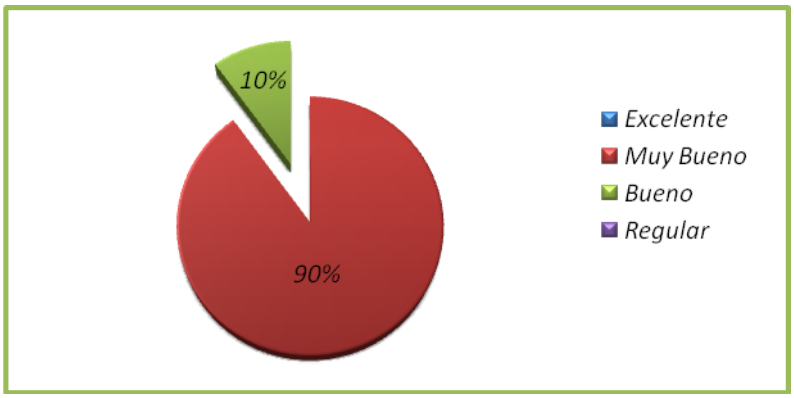
24. ¿Considera usted que la distribución de tablas o representación de resultados es?

Tabla Nº 24

Variable	f	%
Excelente	0	0
Muy Bueno	9	90
Bueno	1	10
Regular	0	0
TOTAL	**10**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 24



Interpretación de resultados

En base a la información recolectada de 10 usuarios/as de la aplicación en el GADCC que representan el 100% del dicha de la población encuestada, y según como se observa en el gráfico, el 90% calificó que la distribución y representación de resultados en las tablas es "Muy Bueno", mientras que el otro 10% restante consideró que la distribución y representación de resultados en las tablas es "Bueno"

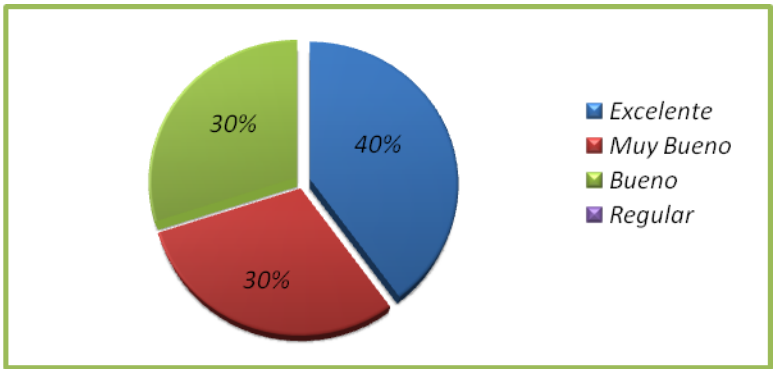
25. ¿Cuál es su criterio referente a las pautas que el sistema le ofrece para que pueda utilizarlo?

Tabla Nº 25

Variable	f	%
Excelente	4	40
Muy Bueno	3	30
Bueno	3	30
Regular	0	0
TOTAL	**10**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 25



Interpretación de resultados

Mediante la encuesta aplicada a 10 usuarios/as de la aplicación en el GADCC que representan el 100% del total de la población, se concluye que el 40% de los encuestados, califica a las pautas de ayuda que el sistema ofrece como "Excelente", mientras que un 30% manifestó que la pautas de ayuda es "Muy Bueno", y el 30% restante de la población encuestada sostuvo que las pautas de ayuda que el sistema ofrece es "Bueno"

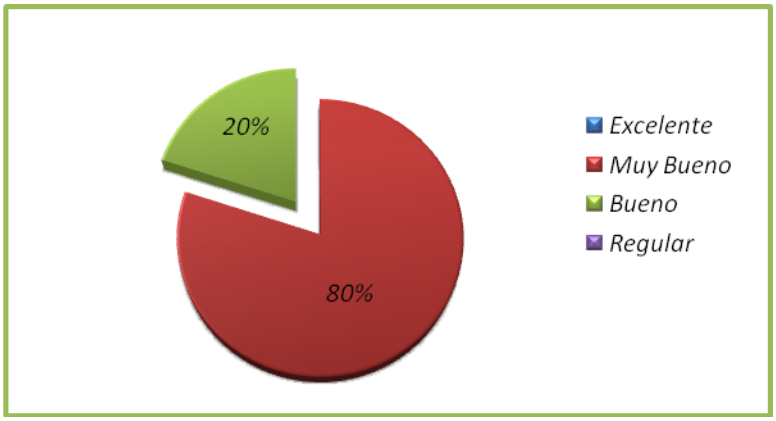
26. ¿Considera usted que las imágenes que el sistema incluye sobre el cantón Calvas es?

Tabla Nº 26

Variable	f	%
Excelente	0	0
Muy Bueno	8	80
Bueno	2	20
Regular	0	0
TOTAL	**10**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 26



Interpretación de resultados

De la información recolectada de 10 usuarios/as de la aplicación en el GADCC que representan el 100% del total de la población encuestada, se concluye que el 80% calificó a las imágenes del cantón Calvas incluidas en la aplicación como "Muy Bueno", mientras que el 20% restante dio una calificación de "Bueno".

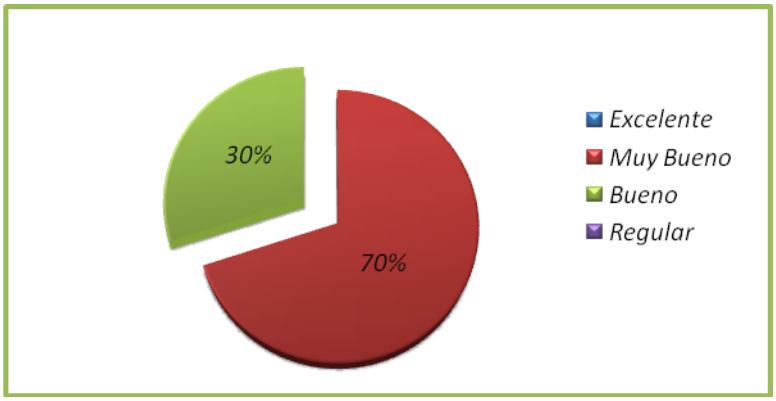
27. ¿Cree usted que la información relacionada con el Municipio de Calvas es?

Tabla Nº 27

Variable	f	%
Excelente	0	0
Muy Bueno	7	70
Bueno	3	30
Regular	0	0
TOTAL	**10**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 27



Interpretación de resultados

En base a la información recolectada de 10 usuarios/as de la aplicación en el GADCC que representan el 100% del dicha de la población encuestada, y según como se observa en el gráfico, se concluye que el 70% calificó a la información relacionada con el Municipio de Calvas como "Muy Bueno", en tanto que el 30% restante le dio una calificación de "Bueno"

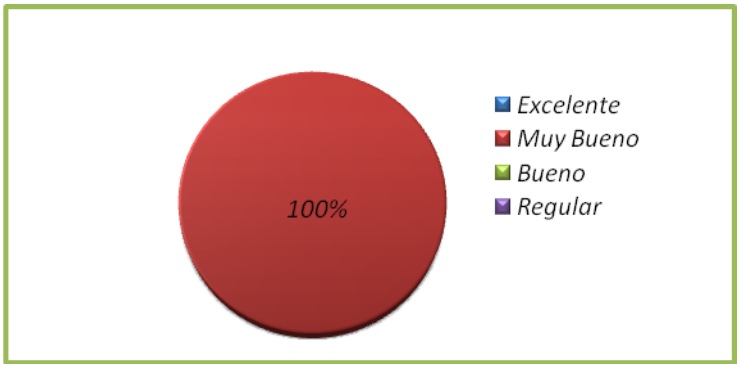
28. ¿Cuándo usted busca información/documentos considera que el resultado es?

Tabla Nº 28

Variable	f	%
Excelente	0	0
Muy Bueno	10	100
Bueno	0	0
Regular	0	0
TOTAL	**10**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 28



Interpretación de resultados

De la información recolectada de 10 usuarios/as de la aplicación en el GADCC que representan el 100% del total de la población encuestada, se concluye que el 100% calificó al resultado de la búsqueda información y/o documentos en la aplicación como "Muy Bueno"

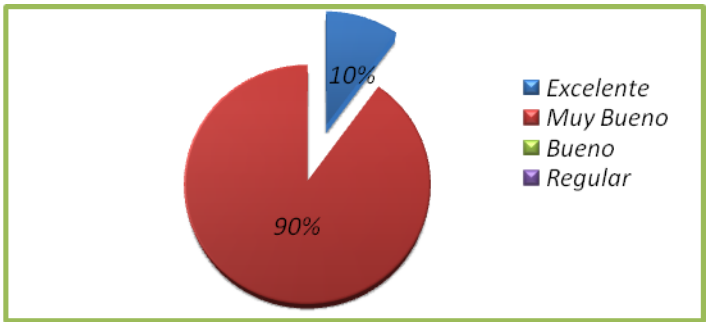
29. ¿Considera usted que la organización de sus documentos es?

Tabla Nº 29

Variable	f	%
Excelente	1	10
Muy Bueno	9	90
Bueno	0	0
Regular	0	0
TOTAL	**10**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 29



Interpretación de resultados

Mediante la encuesta aplicada a 10 usuarios/as de la aplicación en el GADCC que representan el 100% del total de la población, se conoció que el 10% de los encuestados, calificó a la organización de los documentos mediante la aplicación como "Excelente" en tanto que el 90% consideró que la organización de los documentos es "Muy Bueno"

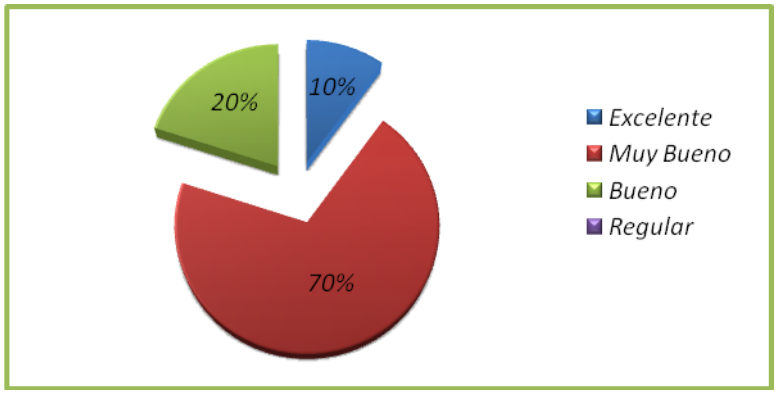
30. ¿Cómo considera usted al proceso de creación de documentos es?

Tabla Nº 30

Variable	f	%
Excelente	1	10
Muy Bueno	7	70
Bueno	2	20
Regular	0	0
TOTAL	**10**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 30



Interpretación de resultados

De la información recolectada de 10 usuarios/as de la aplicación en el GADCC que representan el 100% del total de la población encuestada, se conoció que el 10% de los encuestados, dio una calificación de "Excelente" al proceso de creación de documentos mediante la aplicación, mientras que el 70% de los encuestados consideró que es "Muy Bueno", en tanto que el 20% restante calificó a la creación de documentos mediante la aplicación como "Bueno"

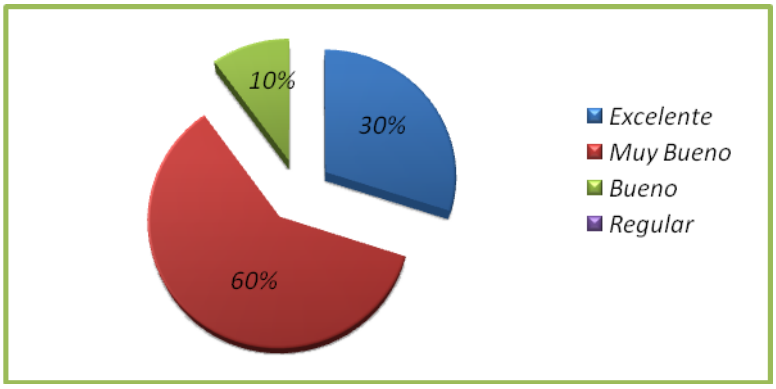
31. ¿Cuándo usted desea enviar un documento, cual es su criterio con respecto a su velocidad?

Tabla Nº 31

Variable	f	%
Excelente	3	30
Muy Bueno	6	60
Bueno	1	10
Regular	0	0
TOTAL	**10**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 31



Interpretación de resultados

En base a la información recolectada de 10 usuarios/as de la aplicación en el GADCC que representan el 100% del de dicha población encuestada, y según como se observa en el gráfico, se concluye que el 30% calificó al el proceso de envió de documentos con respecto a velocidad como "Excelente", mientras que el 60% consideró que es "Muy Bueno", y el 10% restante calificó que la velocidad en el envió de documentos como "Bueno"

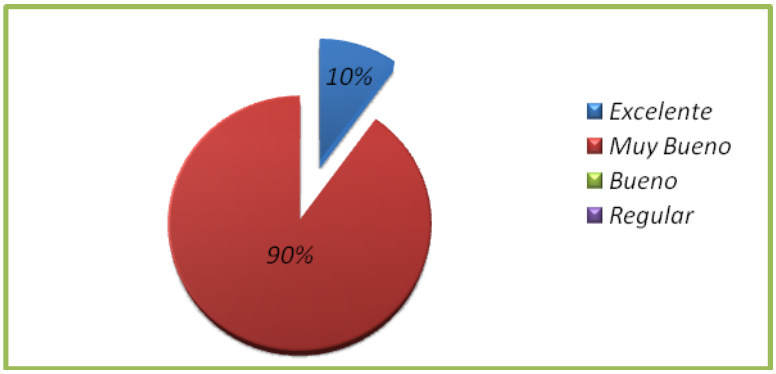
32. ¿Considera usted que cuando guarda o lee información en el sistema, este proceso es?

Tabla Nº 32

Variable	f	%
Excelente	1	10,00
Muy Bueno	9	90,00
Bueno	0	0,00
Regular	0	0,00
TOTAL	**10**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 32



Interpretación de resultados

Mediante la encuesta aplicada a 10 usuarios/as de la aplicación en el GADCC que representan el 100% del total de la población, se conoció que el 10% de los encuestados, calificó como "Excelente" al proceso de guardar y leer información en el sistema, en tanto que el 90% restante considera que el proceso de guardar y leer información en el sistema es "Muy Bueno"

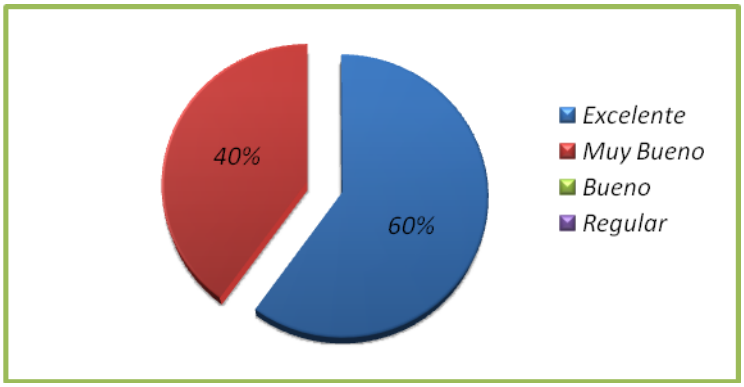
33. Un certificado digital permite que la información que usted envía no sea conocida por el resto de personas, solamente puede leerla su destinatario, para ello se utiliza claves que permiten que el contenido de la información se transforme en un nuevo texto difícil de leer. Por lo tanto **¿Considera usted que el uso de certificados digitales para el envío y recepción de documentos para asegurar seguridad en la información?**

Tabla Nº 33

Variable	f	%
Excelente	6	60
Muy Bueno	4	40
Bueno	0	0
Regular	0	0
TOTAL	**4**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 33



Interpretación de resultados

De la información recolectada de 10 usuarios/as de la aplicación en el GADCC que representan el 100% del total de la población encuestada, se concluye que el 60% calificó al uso de certificados digitales para el envío y recepción de documentos para asegurar seguridad en la información como “Excelente”, mientras que el 40% considera que es “Muy Bueno”.

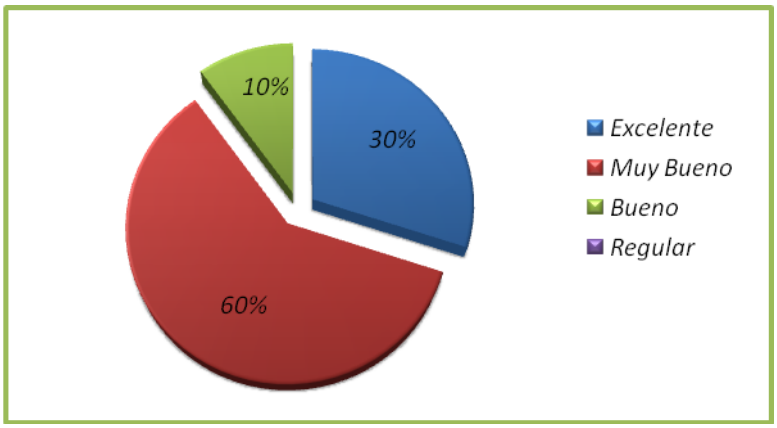
34. ¿Según su criterio cree usted que el dar seguimiento a un documento para tener un mejor conocimiento sobre su tramitación es?

Tabla Nº 34

Variable	f	%
Excelente	3	30
Muy Bueno	6	60
Bueno	1	10
Regular	0	0
TOTAL	**4**	**100**

Fuente: Usuarios/as de la aplicación en el GADCC
Autor: Patricia Chamba y Franklin Andrade

Gráfico Nº 34



Interpretación de resultados

En base a la información recolectada 10 usuarios/as de la aplicación en el GADCC que representan el 100% del de dicha población encuestada, y según como se observa en el gráfico, se concluye que el 30% calificó al proceso de dar seguimiento a un documento para conocer su tramitación como “Excelente”, mientras que el 60% consideró que es “Muy Bueno”, en tanto que 10% le dio una calificación de “Bueno”

ANEXO 7:
ANTEPROYECTO

UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía, las Industrias y los Recursos Naturales no Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

ANTEPROYECTO DE TESIS

"DISEÑO Y CONSTRUCCIÓN DE UN SISTEMA AUTOMATIZADO PARA LA GESTIÓN DE DOCUMENTOS EN LA ILUSTRE MUNICIPALIDAD DEL CANTÓN CALVAS UTILIZANDO CERTIFICADOS DIGITALES"

AUTORES:

Patricia Elizabeth Chamba Briceño
Franklin Freddy Andrade Alverca

LOJA - ECUADOR
2010

ANEXO 7

ANTEPROYECTO

1. TÍTULO

"DISEÑO Y CONSTRUCCIÓN DE UN SISTEMA AUTOMATIZADO PARA LA GESTIÓN DE DOCUMENTOS EN LA ILUSTRE MUNICIPALIDAD DEL CANTÓN CALVAS UTILIZANDO CERTIFICADOS DIGITALES"

2. PROBLEMÁTICA

2.1. SITUACIÓN PROBLÉMICA

La incorporación de nuevas tecnologías de la información, hace que, en muchas ocasiones los conceptos tradicionales resulten poco idóneos para interpretar las nuevas realidades que van enfocadas a las necesidades de la sociedad actual. El avance de su implantación en todas las actividades ha provocado cambios de tal magnitud que la sociedad actual está inmersa en la era de la revolución informática. Este avance nos permite acceder a todo tipo de información y obtener con ello el beneficio correspondiente.

La información es calificada como uno de los factores más influyentes que dirigen el rumbo de cualquier organización; Por ello es recomendable dejar de lado el uso de técnicas de gestión tradicionales en el ámbito administrativo, ya que esto, ocasiona inconvenientes como: retrasos en la entrega de información, pérdida de tiempo en la búsqueda de algún documento, confusiones, desorganización y demás incidentes que pueden afectar el cumplimiento de actividades dentro de las instituciones. Las instituciones ya sea de carácter público o privado, persiguen el cumplimiento de sus objetivos los mismos que se encuentran encaminados hacia aspectos comerciales, industriales y prestación de servicios, razón por la cual disponen de volúmenes de información considerables, debido a ello es que, para facilitar su ejecución requieren de mecanismos automatizados encargados de suministrar dicha información.

La Ilustre Municipalidad de Calvas se encuentra inmersa dentro de estos aspectos, ya que la información que se tramita para llegar a su destinatario debe pasar por varios

departamentos, situación que ocasiona que existan posibles alteraciones del contenido de los documentos por personal no autorizado, sin que se pueda identificar a los involucrados que participaron en este hecho. La información que se tramita está relacionada con aspectos tales como: actas de sesiones, ordenanzas, resoluciones, convenios, órdenes de pago, solicitudes de los departamentos, boletines de prensa, oficios recibidos y enviados, procesos de contratación (contrataciones, licitaciones, calificaciones), contratos de obras ejecutadas, leyes y registros oficiales; motivo por cual es necesario que se automatice el tratamiento de dichos documentos con la finalidad de que estos sea veraces, precisos, confiables y estén disponibles en el momento que se los requiera. De igual manera es necesario el utilizar mecanismos encargados de garantizar la seguridad e integridad de los documentos al momento de su creación, acceso y traslado, uno de ellos lo constituyen las firmas digitales, encargadas de la autentificación de los mismos, asegurando a su destinatario tanto la identidad de la persona que lo envía como la integridad de dicho documento, todo este proceso está basado en algoritmos de encriptación que consisten en convertir un texto legible en otro ilegible, es decir los documentos de codifican y solo pueden ser leídos si se dispone de la clave que ha sido asignada para llevar a cabo su tramitación.

La obtención y uso de claves públicas y privadas se logra gracias a las entidades certificadoras reconocidas por la ley. En nuestro país el Banco Central del Ecuador está destinado para llevar a cabo este fin, el cual fue acreditado por el Consejo Nacional de Telecomunicaciones (CONATEL) mediante resolución Nª 481-20-2008 el 8 de Octubre del 2008. Los certificados digitales vinculan una identidad a un par de claves electrónicas (públicas y privadas) que pueden ser usadas para encriptar y firmar información digital, proporcionado de esta manera una solución de seguridad más completa ya que asegura la identidad de todas las partes involucradas durante la tramitación de un documento entre un departamento y otro.

Es por ello que considerando todos los aspectos mencionados anteriormente, hemos planteado el desarrollo de un proyecto de tesis denominado “DISEÑO Y CONSTRUCCIÓN DE UN SISTEMA AUTOMATIZADO PARA LA GESTIÓN DE DOCUMENTOS EN LA ILUSTRE MUNICIPALIDAD DEL CANTÓN CALVAS UTILIZANDO CERTIFICADOS DIGITALES” el mismo que pueda ser usado como una herramienta de apoyo para brindar la seguridad, confidencialidad e integridad necesaria

de los documentos que se tramitan en los diferentes departamentos que conforman esta institución.

2.2. PROBLEMA GENERAL

"La falta de un sistema automatizado que disponga de niveles de seguridad que garanticen la gestión de documentos tanto en su recepción como en su envió en la Ilustre Municipalidad del cantón Calvas, ocasiona que se brinde un servicio de baja calidad e inseguro durante la tramitación de documentos en esta institución"

2.3. DELIMITACIÓN

El Ilustre Municipio del cantón Calvas de la provincia de Loja, es una institución que dispone de un volumen de información significativa, proveniente de cada uno de sus departamentos tal y como lo es la tramitación de documentos, los cuales son emitidos por la ciudadanía, por entidades externas, y por la misma institución. Considerando estas pautas es que el sistema automatizado de gestión de documentos, será desarrollado en base a dicha información, utilizando firmas digitales, esto con la finalidad de que exista mayor seguridad, confidencialidad y autenticación de la documentación tanto recibida como enviada y así evitar que exista manipulación no autorizada de la misma.

La documentación que se maneja tiene que ver con: Actas de sesiones, ordenanzas, resoluciones, convenios, órdenes de pago, solicitudes de los departamentos, boletines de prensa, oficios recibidos y enviados, procesos de contratación (contrataciones, licitaciones, calificaciones), contratos de obras ejecutadas, leyes y registros oficiales.

Tomando en cuenta todos estos aspectos es que hemos decidido establecer que nuestro Sistema Automatizado de Gestión de Documentos debe contar con los siguientes módulos:

- Módulo de gestión de documentos.
- Módulo de administración de usuarios.
- Módulo de consulta general.
- Módulo de respaldo general de documentos.
- Módulo de auditoría del sistema.

2.3.1. PROBLEMAS ESPECÍFICOS DE INVESTIGACIÓN

La Ilustre Municipalidad del cantón Calvas es una institución en la que el proceso de envió y recepción de documentos entre un departamento y otro se efectúa sin tomar medidas de seguridad necesarias para asegurar que dicha documentación llegue a su destinario de manera íntegra y sin alteraciones. Es por ello que tomando en cuenta estos factores es que hemos definido la existencia de los siguientes problemas que afectan el normal cumplimiento de las actividades en esta institución, los cuales son:

- Desorganización de la información existente en cada uno de los departamentos pertenecientes al Municipio del cantón Calvas.
- Inexistencia de certificados digitales encargados de asegurar la integridad de los documentos que se tramitan en los diferentes departamentos del Municipio de Calvas.
- Falta de seguridad durante el acceso al contenido de los documentos en estado de tramitación o que ya han sido tramitados.
- Falta de utilización de claves públicas y privadas emitidas por entidades de certificación, en las huellas digitales que hayan sido obtenidas.
- Falta de control y seguridad en el acceso y utilización de los módulos del sistema.
- Falta de control y seguridad en el acceso a personal no autorizado durante la utilización del sistema de gestión de documentos.

2.3.2. ESPACIO

El sistema de Gestión de Documentos se desarrollará en el cantón Calvas, provincia de Loja, específicamente en la Ilustre Municipalidad del cantón Calvas, debido a que es una institución pública encargada de velar por los intereses de sus habitantes y por lo tanto debe prestar sus servicios de manera eficiente.

De igual manera la tramitación de información que en esta institución se realiza es extensa; en algunos casos debe pasar de un departamento a otro hasta finalmente llegar

a su destinario, dicha documentación tiene que ver con lo relacionado a: Actas de sesiones, ordenanzas, resoluciones, convenios, órdenes de pago, solicitudes de los departamentos, boletines de prensa, oficios recibidos y enviados, procesos de contratación (contrataciones, licitaciones, calificaciones), contratos de obras ejecutadas, leyes y registros oficiales, hechos por los cuales resulta necesaria su automatización.

2.3.3. TIEMPO

El proyecto de tesis denominado "Diseño y construcción de un sistema automatizado para la gestión de documentos en la Ilustre Municipalidad del cantón Calvas utilizando certificados digitales", será desarrollado en un plazo máximo de ocho meses equivalente a 170 días, el cual está estipulado desde el día 6 de abril hasta el 10 de diciembre del presente año, para lo cual cada una de las tareas se las clasificado en base a las etapas correspondientes al Proceso de Ingeniería de Software, de tal manera que se facilite su ejecución.

2.3.4. UNIDADES DE OBSERVACIÓN

Para el desarrollo del presente proyecto de tesis, será necesaria la investigación de información que complete su estudio, de manera tal que se logre cumplir con los objetivos que se han establecido al inicio. Es por ello que las unidades de observación necesarias serán:

- Sistemas de gestión de documentos
- Firma digital
- Seguridad de la información.
- Seguridad del software.
- Auditoria informática
- Ilustre Municipio de Calvas

3. JUSTIFICACIÓN

3.1. JUSTIFICACIÓN

La Universidad Nacional de Loja con el afán de seguir siendo una de las pioneras y una de las más importantes en la Región Sur del País, ha venido forjando profesionales acordes a las necesidades que requiere la sociedad actual, es por eso, que se ven en la

responsabilidad de ir mejorando de manera paulatina el crecimiento y desarrollo intelectual de cada uno de los miembros que conforman está gran comunidad universitaria.

Esta institución de educación superior con una amplia trayectoria y experiencia siguiendo con su objetivo de formar profesionales capaces de enfrentar los grandes retos dentro de un ente social lleno de varios tipos de problemas los cuales afectan de manera directa al desarrollo sustentable de la sociedad en la cual habitamos, tiene incorporada la carrera de Ingeniería de Sistemas, destinada a la solución de tales problemas. Es por ello que, enmarcándonos dentro de los aspectos antes mencionados es que se ha creído conveniente el realizar un proyecto de tesis denominado ***"****Diseño y construcción de un sistema automatizado para la gestión de documentos en la Ilustre Municipalidad del cantón Calvas utilizando certificados digitales"* el mismo que se encargará de garantizar la seguridad e integridad de los diferentes documentos que se tramitan en esta institución, de manera tal que puedan llegar a su destino de manera completa e íntegra.

De igual manera con el uso de firmas digitales se elimina el riesgo de pérdida y deterioro de documentos, permitiendo también que exista una mayor facilidad en cuanto a su acceso, una de las alternativas para conseguir este propósito es mediante la automatización de dicha información; pero conservando políticas de seguridad tales como la encriptación y filtrado de accesos, logrando con ello que la información que se envíe pueda llegar de manera segura a nuestro destinatario y se verifique además que el remitente del mensaje o quien está utilizando los datos sea el correcto.

Justificación Académica

El presente trabajo se justifica a nivel académico debido a que nos basaremos en la aplicación tanto de técnicas como de métodos que han sido impartidos a lo largo del proceso de enseñanza – aprendizaje, y en el modelo pedagógico denominado Sistema Académico Modular por Objetos de Transformación, SAMOT, el cual tiene como propósito principal que los estudiantes pongan en práctica los conocimientos que hayan sido adquiridos en su formación académica, y de esta manera cumplir con los objetivos definidos en el presente proyecto; mismo que representará un gran aporte para una institución que busca no solo la eficiencia y eficacia en la tramitación de documentos que se manejan en los diferentes departamentos, sino también el bienestar de sus

ciudadanos. La Ilustre Municipalidad del cantón Calvas se constituye en una institución que persigue tales propósitos.

Por otro lado enfocándonos desde el punto de vista académico, el desarrollo del presente proyecto de tesis nos permitirá a nosotros como estudiantes el obtener el título de Ingenieros en Sistemas.

Justificación Económica

Para la realización y cumplimiento de los objetivos previstos en el presente proyecto de tesis, es necesario el disponer de recursos económicos, tanto para su construcción como para su implementación. Por ello es que, los gastos que demanda el proceso de construcción del *Sistema automatizado para la gestión de documentos en la Ilustre Municipalidad del cantón Calvas utilizando certificados digitales,* serán financiados con recursos propios del grupo de desarrolladores del mismo.

Justificación Técnica

El avance tecnológico hoy en día contribuye notablemente en el mejoramiento de la calidad de vida de todas las personas, tanto los equipos de cómputo y telecomunicaciones, como los sistemas informáticos, son los encargados de complementar la optimización de recursos durante el cumplimiento de una actividad o proceso. Considerando estos aspectos es que resulta factible la realización del presente proyecto de tesis, en el cual se necesitan tanto equipos de cómputo como herramientas de software libre para su desarrollo tales como: lenguaje de programación Java, programas de diseño y codificación, entre otros.

Justificación Operativa

El desarrollo del sistema automatizado para la gestión de documentos utilizando firmas digitales es posible, ya que las personas involucradas colaborarán desinteresadamente en su realización, además el personal que labora en cada uno de los departamentos aceptarán y se relacionarán con el funcionamiento del sistema, puesto que les permitirá trabajar de manera más eficiente resolviendo inconvenientes en cada una de las actividades que desempeñan.

Justificación Social

El proponer alternativas de solución a los problemas que hoy en día aquejan a nuestra sociedad, es uno de los aspectos en los que se debe tener énfasis a la hora de desarrollar un proyecto. Es por ello que el desarrollo del sistema automatizado para la gestión de documentos utilizando certificados digitales, constituye una de las pautas para aportar significativamente a nuestro entorno y a la vez dar solución a los inconvenientes que actualmente se evidencian en la Ilustre Municipalidad de Calvas.

3.2. VIABILIDAD

El desarrollo del proyecto de tesis denominado **"**Diseño y construcción de un sistema automatizado para la gestión de documentos en la Ilustre Municipalidad del cantón Calvas utilizando certificados digitales", dispone de factibilidad debido a que dará solución a los inconvenientes que actualmente se presentan en esta institución durante la tramitación de documentos ya sea en su envío o recepción, permitiendo además que se cuente con medidas de seguridad necesarias para acceder al contenido de ésta información.

Por otra parte, la disponibilidad de los equipos de cómputo tanto de software como de hardware es un factor que incide notablemente para que su ejecución se lleve a cabo de acuerdo a lo planificado, así mismo dichos equipos cumplen con las características técnicas requeridas lo cual permitirá que el resultado sea el esperado.

Los usuarios juegan un papel muy importante en la aceptación de un determinado sistema, razón por la cual será necesario que éste disponga de las facilidades de uso necesarias y por lo tanto su rendimiento se vea reflejado en los resultados arrojados por el mismo. Los recursos económicos que demanda todo el proceso de construcción del Sistema de Gestión de Documentos serán solventados por parte de sus desarrolladores, y en caso de que la institución amerite su implementación, los gastos correrán por cuenta de la Municipalidad de Calvas.

Cabe recalcar que el Sistema de Gestión de Documentos, constituye un aporte significativo a nuestra sociedad, ya que dará solución a diferentes inconvenientes que provocan que actividades ya planificadas no puedan ser cumplidas de manera satisfactoria en esta institución.

4. OBJETIVOS

4.1. GENERAL

"Diseñar y construir un sistema automatizado para la gestión de documentos en la Ilustre Municipalidad del cantón Calvas utilizando certificados digitales".

4.2. ESPECÍFICOS

- ✓ Organizar los documentos de acuerdo a su índole de manera que se garantice eficiencia y eficacia durante su acceso.
- ✓ Generar certificados de autenticación que permitan firmar digitalmente la información que se enviará y recibirá entre los diferentes departamentos que conforman la institución
- ✓ Usar funciones hash para generar datos asociados (huella digital) basados en la encriptación asimétrica o codificación de los documentos digitales.
- ✓ Aplicar claves privadas al documento original para obtener la firma digital que se enviará.
- ✓ Auditar cada una de las acciones realizadas en los módulos que conforman el sistema.
- ✓ Establecer e implantar niveles de seguridad y acceso en la aplicación que permitan el acceso únicamente a personal autorizado.

5. MARCO TEÓRICO

CAPITULO I: SISTEMAS DE GESTIÓN DE DOCUMENTOS

1.1. Objetivos.

Un sistema de gestión de documentos es aquel sistema software que provee servicios a los usuarios y aplicaciones en el uso de archivos. El único camino que tiene el usuario o la aplicación para acceder a los archivos es a través de un sistema de gestión de documentos. Sus objetivos son:

- Cumplir con las necesidades de gestión de datos y con los requisitos del usuario, que incluye el almacenamiento de, datos y la capacidad de ejecutar las operaciones en la lista precedente.
- Garantizar, en la medida de lo posible, que el dato en el archivo es válido.
- Optimizar el rendimiento, ambos desde el punto de vista del sistema en términos de productividad global, y como punto de vista del usuario en tiempos de respuesta.
- Para proveer soporte de E/S para una variedad de tipos de dispositivos de almacenamiento.
- Para minimizar o eliminar la posibilidad de pérdida o destrucción de datos.
- Para proveer un conjunto estándar de rutinas de E/S.
- Para proveer soporte de E/S para múltiples usuarios, en caso de sistemas multiusuario.

1.2. Arquitectura.

Una manera de hacerse una idea del alcance de la gestión de documentos es observar una representación de una organización típica del software. En el nivel más bajo se encuentran los gestores de dispositivos que se comunican directamente con los dispositivos periféricos o sus controladores o canales. En operaciones con archivos, los dispositivos típicos controlados son discos y unidades de cinta. Los gestores de dispositivos son considerados generalmente como parte del sistema operativo.

El siguiente nivel es conocido con el nombre de **sistema de documentos básico o nivel de E/S física**, este sistema se encarga de ubicar los bloques de datos en el dispositivo de almacenamiento secundario y además del almacenamiento intermedio de los mismos en

la memoria principal. El sistema de archivos básico se considera a menudo parte del sistema operativo.

El supervisor básico de E/S es el responsable de la iniciación y terminación de toda la E/S de documentos. En este nivel se mantienen unas estructuras de control que se encargan de la E/S con los dispositivos, la planificación y el estado de los documentos. El supervisor básico de E/S es parte del sistema operativo.

La E/S lógica es la parte del sistema de archivos que permite a usuarios y aplicaciones acceder a los registros. Así, mientras el sistema de archivos básico trabaja con bloques de datos, el módulo de E/S lógica lo hace con registros.

Finalmente, el nivel del sistema de archivo más cercano al usuario es, generalmente, el **método de acceso**. Los diferentes métodos de acceso reflejan las distintas estructuras de documentos y las formas diferentes de acceder y procesar los datos.

1.3. Funciones.

Los usuarios y las aplicaciones interactúan con el sistema de gestión de documentos mediante comandos para crear y borrar archivos y realizar operaciones sobre los documentos. Antes de ejecutar alguna operación, los archivos del sistema deben identificar y localizar el documento seleccionado. Esto requiere el uso de alguna clase de directorio que es reservado para describir la localización de todos los documentos, más sus atributos. Además**,** la mayoría de los sistemas compartidos aplican algún control de acceso a los usuarios: solamente los usuarios autorizados están permitidos para acceder a documentos particulares en determinados lugares. El usuario o la aplicación ve al documento con una estructura que organiza los registros, como una estructura secuencial. De este modo, para traducir las órdenes del usuario a órdenes específicas de manipulación de documentos, debe emplearse el método de acceso apropiado para esta estructura de documentos.

1.4. Acceso a los Documentos

Se refiere al método utilizado para acceder a los registros de un archivo o documento prescindiendo de su organización. Existen distintas formas de acceder a los datos:

Secuenciales.- Los registros se leen desde el principio hasta el final del archivo, de tal forma que para leer un registro se leen todos los que preceden.

Directo.- Cada registro puede leerse / escribirse de forma directa solo con expresar su dirección en el fichero por él numero relativo del registro o por transformaciones de la clave de registro en él numero relativo del registro a acceder.

Por Índice.- Se accede indirectamente a los registros por su clave, mediante consulta secuenciales a una tabla que contiene la clave y la dirección relativa de cada registro, y posterior acceso directo al registro.

Dinámico.- Es cuando se accede a los archivos en cualquier de los modos anteriormente citados.

La elección del método está directamente relacionada con la estructura de los registros del archivo y del soporte utilizado.

1.5. Organización de los Documentos.

Los archivos o documentos se encuentran organizados lógicamente como una secuencia de registros de varias longitudes diferentes.

Los registros de longitud fija.- Son los que almacenan la información en los archivos mediante un encabezado y luego se introducen uno a uno los registros ubicados en posiciones consecutivas.

Los registros de longitud variable.- Es el almacenamiento de registros de varios tipos en un archivo y permite uno o más campos de longitudes variables y dichos campos pueden ser repetidos. La longitud de los registros debe estar definida correctamente para poder leer y escribir de forma efectiva.

1.5.1. Enfoques Generales para la Organización de Documentos

Los enfoques son:

- **Enfoque de acceso secuencial:** Se refiere al procesamiento de los archivos o documentos de acuerdo con el orden específico. Ejemplo : Archivos secuenciales y de texto.
- **Enfoque de acceso Directo** Permite recuperar registros individuales sin leer otros registros del archivo o documento.

1.6. Estructura.

La manera en que la información se almacena difiere mucho en los diferentes sistemas. Parte de la información puede almacenarse en un registro de cabecera asociado al archivo, esto reduce el espacio necesario para el directorio, haciendo más fácil mantener todo el directorio.

La forma más fácil de estructuración de un directorio es una lista de entradas, unas para cada archivo o documento. Esta estructura puede representarse con un simple archivo secuencial, con el nombre del archivo haciendo las veces de clave.

Operaciones que se pueden realizar con un directorio

- **Buscar.-** Cuando alguien referencia el archivo, debe buscarse en el directorio la entrada correspondiente al archivo.
- **Crear archivo.-** Al crear un nuevo archivo debe añadirse una entrada al directorio.
- **Borrar archivo**.- Al borrar un archivo, debe eliminarse una entrada al directorio.
- **Listar directorio.-** Puede solicitarse todo el directorio o una parte.

Una simple lista no se ajusta bien a estas operaciones. Si el directorio es una simple lista de secuencias, no ofrecerá ayuda en la organización de los archivos y obligará al usuario a tener cuidado de no usar el mismo nombre para dos tipos diferentes de archivos. Para resolver este problema se puede acudir a un esquema de dos niveles donde hay un directorio para cada usuario y un directorio maestro. Un método más potente y flexible es el directorio jerárquico o estructurado en árbol. Existe un directorio maestro que contiene un número determinado de directorios de usuario. Cada uno de estos directorios puede tener a su vez subdirectorios y archivos como entradas. Esto se cumple en cualquier nivel.

Para organizar cada directorio y subdirectorio. El método más simple es almacenar cada directorio como un archivo secuencial. Cuando los directorios contengan un número muy grande de entradas, tal organización puede conducir a tiempos de, búsqueda innecesariamente grandes. En ese caso se prefiere una estructura de dispersión.

1.7. Compartimiento de Documentos.

En un sistema multiusuario, casi siempre existe la necesidad de permitir a los usuarios compartir archivos o documentos. Dos problemas surgen:

- Los derechos de accesos
- Gestión de los accesos simultáneos

Derechos de Acceso

El sistema de archivos o documentos provee una herramienta flexible para permitir compartir extensos archivos entre los usuarios. El sistema de archivos o documentos debe proporcionar un numero de opciones de modo en que un archivo que es accedido pueda ser controlado. Normalmente, al usuario o a los grupos de usuarios se les otorgan ciertos derechos de acceso a cada archivo. La siguiente lista representa los derechos de acceso que pueden ser asignados a un usuario en particular para un archivo en particular:

Ninguno.- El usuario no puede siquiera determinar la existencia del archivo ni mucho menos acceder al mismo. No se permite al usuario leer el directorio de usuario que incluya al archivo o documento.

Conocimiento.- El usuario sabe de la existencia del archivo o documento y quien es el dueño. El usuario puede solicitar los derechos de acceso adicionales al propietario.

Ejecución.- El usuario puede ejecutar y cargar un programa pero no copiarlo.

Lectura.- El usuario puede leer el archivo para cualquier propósito, incluyendo copia y ejecución.

Adición.- El usuario puede añadir datos al archivo o documento, generalmente al final, pero no puede modificar o borrar el contenido del mismo.

Actualización.- El usuario puede modificar, borrar y añadir otros datos al archivo.

Cambio de protección.- El usuario puede cambiar los derechos de acceso otorgados a usuarios.

Borrado.- El usuario puede borrar el archivo del sistema de archivos.

Los derechos constituyen una jerarquía. Si un usuario adquiere el derecho de la actualización para un archivo determinado, también habrá adquirido los derechos siguientes: conocimiento, ejecución, lectura y adición.

El propietario de un archivo o documento dispone de los derechos de acceso listados antes y puede otorgar derechos a los otros. Puede ofrecerse acceso a las siguientes clases de usuarios:

- **Usuario específico.-** Usuarios individuales quienes son designados por su ID de usuario.
- **Grupos de usuarios.-** Un conjunto de usuarios no definidos individualmente.
- **Todos.-** Todos los usuarios que tengan acceso al sistema. Estos serán archivos públicos.

Acceso Simultáneo

Cuando el acceso es concedido para añadir o actualizar un archivo o documento a más de un usuario, el sistema operativo o el sistema de gestión de documentos debe hacer cumplir una disciplina. Un método de fuerza bruta consiste en permitir a los usuarios bloquear el archivo entero cuando lo vaya a actualizar. Un mejor control es bloquear los registros individuales durante la actualización. Al disertar la posibilidad de accesos comparados, deben abordarse aspectos de exclusión mutua e interbloqueo.

CAPITULO II: FIRMA DIGITAL

2.1. Definición

La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos gocen de una característica que únicamente era propia de los documentos en papel. Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje.

La firma digital no implica asegurar la confidencialidad del mensaje; un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma holográficamente.

La firma digital es un instrumento con características técnicas y normativas. Esto significa que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen.

Las firmas digitales deben tener las mismas propiedades que las escritas:

- **Únicas.** Una firma digital debe de ser generada únicamente por su usuario.
- **No se podrán falsificar.** La generación por parte de otros usuarios de firmas de cara a falsificar una firma digital será imposible, es decir tendrán que resolver problemas intratables de una gran complejidad mientras intentan falsificas la firma

2.2. Funcionamiento

La firma digital de un documento no es un passwords, es el resultado de aplicar cierto algoritmo matemático, denominado función hash, al contenido.

Esta función asocia un valor dentro de un conjunto finito (generalmente los números naturales) a su entrada. Cuando la entrada es un documento, el resultado de la función es un número que identifica casi unívocamente al texto.

Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido.

Funciones Hash

Para poder realizar una firma digital, es necesario primero convertir el mensaje en un Número. Este Número es entregado a la función de Hash, que produce el resumen del mensaje. Esta función convierte un número grande (el mensaje) en un número pequeño (el resumen). Para que esto funcione, no debería ser sencillo encontrar dos mensajes que produjeran el mismo resumen. Si se pudiera hacer, podrías cambiar el mensaje correspondiente a una firma, como aquel banco que cambió páginas internas del contrato.

El número pequeño del resumen suele tener una longitud de 128 bits (MD5), o de 160 bits (SHA-1). Cada BIT puede ser tanto un "0" como un "1". Por lo tanto existen 2 elevado a 128 posibles resúmenes de 128 bits de largo, o 2 elevado a 160 resúmenes de 160 bits.

Ahora bien, el proceso de obtención del resumen a partir del mensaje debe ser determinístico. Debe ser repetible. El mismo mensaje siempre debe dar el mismo resumen. Si no, el proceso de verificación no funcionaría.

Pero, al mismo tiempo, la salida de la función de hash debe parecer aleatoria. Debería resultar imposible obtener el mensaje a partir del resumen. De otra manera, alguien

podría obtener varios mensajes que tendrían el mismo resumen. Para que una función de hash sea buena, debe ser una función unidireccional. Debe funcionar en un sentido, pero no en el contrario. Además debe ser muy difícil encontrar dos mensajes diferentes que produzcan el mismo resumen.

Cuando ya dispone del resumen del mensaje, el número pequeño, debe firmarlo (cifrarlo). Esto también involucra una transformación matemática. Un algoritmo efectivo debe hacer uso de un sistema de clave pública para cifrar sólo la firma. En particular, el valor "hash" se cifra mediante el uso de la clave privada del firmante, de modo que cualquiera pueda comprobar la firma usando la clave pública correspondiente. El documento firmado se puede enviar usando cualquier otro algoritmo de cifrado, o incluso ninguno si es un documento público.

El proceso de firma es el siguiente:

- El usuario prepara el mensaje a enviar.
- El usuario utiliza una función hash segura para producir un resumen del mensaje.
- El remitente encripta el mensaje original con su clave privada. La clave privada es aplicada al texto usando un algoritmo matemático.
- El remitente envía electrónicamente el mensaje encriptado, y el hash generado.
- El destinatario usa la clave pública del remitente para verificar la firma digital, es decir para desencriptar el mensaje original.
- El destinatario realiza un resumen del mensaje desencriptado utilizando la misma función resumen segura.
- El destinatario compara los dos resúmenes. Si los dos son exactamente iguales el destinatario sabe que los datos no han sido alterados desde que fueron firmados.

2.2.1. Proceso de Firma y Verificación de Firma

En el siguiente ejemplo, se describe el proceso de la firma y verificación de firma, para el envío y recepción de un correo electrónico: Recordemos que Juan y Mario tienen sus pares de claves correspondientes, como se observa en la Fig N° 2.1.

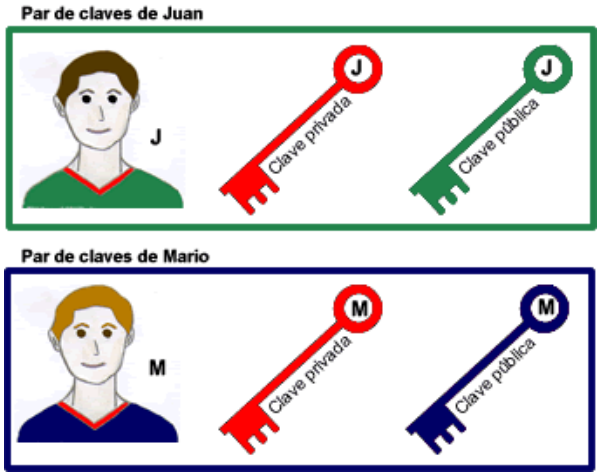


Fig N° 2.1. Par de claves asignadas a las personas involucradas en la comunicación

Proceso de Firma

Juan escribe un correo electrónico a Mario. Es necesario que Mario pueda verificar que es Juan quien ha enviado el correo. Por ello, Juan debe enviar el correo firmado digitalmente.

Cuando Juan le indica al programa de correo que envíe el mensaje firmado digitalmente, éste realizará las siguientes operaciones, detalladas en la Fig N°2.2.

- Procesa el mensaje mediante una función hash y obtiene la huella digital (número) o resumen.
- Cifra el resumen utilizando la clave privada que Juan ingresa. Como resultado se obtiene la firma digital del mensaje.
- Envía a Mario el mensaje original junto con la firma digital del mensaje y la correspondiente clave pública.

Verificación de Firma

Mario recibe el correo junto con la firma digital. Tiene que comprobar la validez de la misma para dar por bueno el mensaje y reconocer al autor (integridad y autenticación).

En el momento que Mario recibe el mensaje, el programa de correo electrónico realizará las siguientes operaciones, detalladas en la Fig. N° 2.2.

- Descifra la firma digital con la clave pública recibida de parte de Juan y obtiene el número de hash (huella digital o resumen) original producido por Juan.
- Aplica al mensaje recibido la función hash para obtener una huella digital o resumen.
- Compara la huella digital recibida con la obtenida en el punto anterior. Si son iguales, Mario podrá estar seguro de que quien ha enviado el mensaje es Juan y que el mismo no ha sido modificado. Si son diferentes entonces significa que el mensaje ha sufrido alguna alteración posterior al envío. Con este sistema conseguimos:

Autenticación: la firma digital es equivalente a la firma manuscrita de un documento.

Integridad: el mensaje no podrá ser modificado.

No repudio en origen: el emisor no puede negar haber enviado el mensaje.

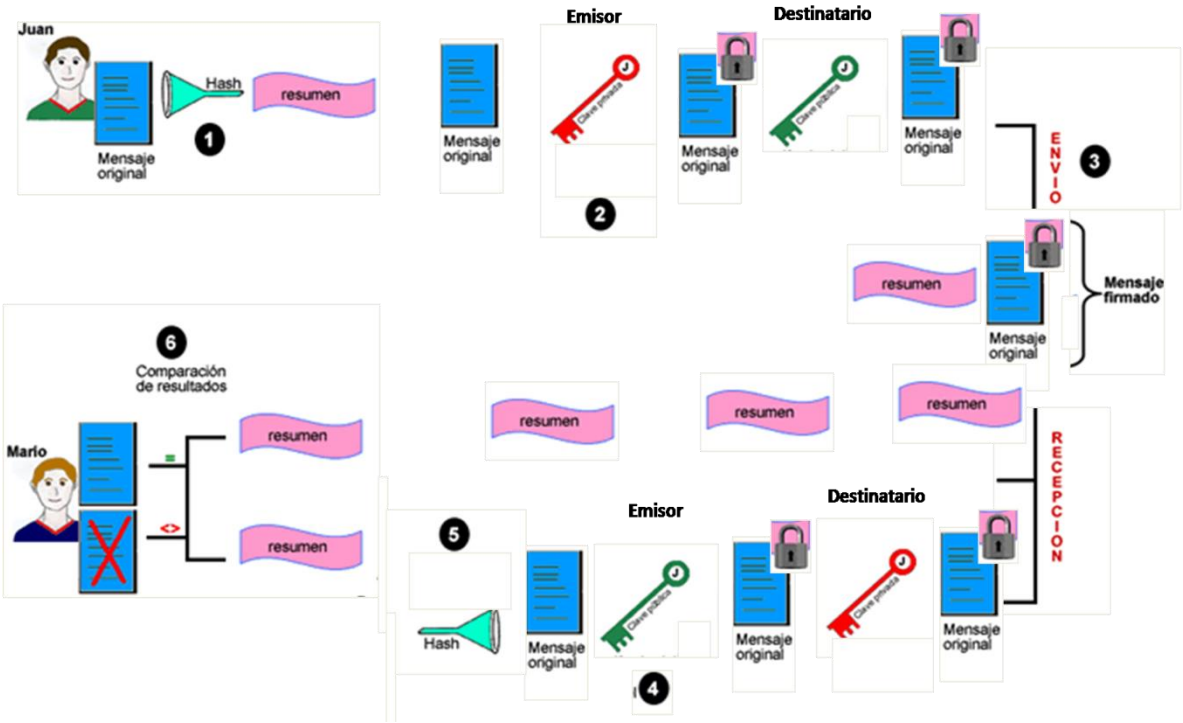


Fig. N° 2.2. Proceso de firma y verificación de firma

2.2.2. Valor Legal

Para la legislación argentina los términos "Firma Digital" y "Firma Electrónica" no poseen el mismo significado. La diferencia radica en el valor probatorio atribuido a cada uno de ellos, dado que en el caso de la "Firma Digital" existe una presunción "iuris tantum" en su favor; esto significa que si un documento firmado digitalmente es verificado correctamente, se presume salvo prueba en contrario que proviene del suscriptor del certificado asociado y que no fue modificado. Por el contrario, en el caso de la firma electrónica, de ser desconocida por su titular, corresponde a quien la invoca acreditar su validez. Por otra parte, para reconocer que un documento ha sido firmado digitalmente se requiere que el certificado digital del firmante haya sido emitido por un certificador licenciado (o sea que cuente con la aprobación del Ente Licenciante).

Es por esto que, si bien entendemos que en los ambientes técnicos se emplea habitualmente el término Firma Digital para hacer referencia al instrumento tecnológico, independientemente de su relevancia jurídica, solicitamos a todos los proveedores de servicios de certificación, divulgadores de tecnología, consultores, etc. que empleen la denominación correcta según sea el caso a fin de no generar confusión respecto a las características de la firma en cuestión.

La legislación argentina emplea el término "Firma Digital" en equivalencia al término "Firma Electrónica Avanzada" utilizado por la Comunidad Europea o "Firma Electrónica" utilizado en otros países como Brasil o Chile.

2.2.3. Tipos

Según la ley de firma digital, que puede ser diferente en cada país, define tres tipos de firma digital:

- **Simple:** incluye un método de identificar al firmante.
- **Avanzada:** además de identificar al firmante permite garantizar la integridad del documento. Se emplean técnicas de PKI.
- **Reconocida:** es la firma avanzada ejecutada con un DSCF (dispositivo seguro de creación de firma) y amparada por un certificado reconocido (certificado que se otorga tras la verificación presencial de la identidad del firmante).

2.3. Claves Privadas y Públicas

En la elaboración de una firma digital y en su correspondiente verificación se utilizan complejos procedimientos matemáticos basados en criptografía asimétrica (también llamada criptografía de clave pública).

En un sistema criptográfico asimétrico, cada usuario posee un par de claves propio. Estas dos claves, llamadas clave privada y clave pública, poseen la característica de que si bien están fuertemente relacionadas entre sí, no es posible calcular la primera a partir de los datos de la segunda, ni tampoco a partir de los documentos cifrados con la clave privada.

El sistema opera de tal modo que la información cifrada con una de las claves sólo puede ser descifrada con la otra. De este modo si un usuario cifra determinada información con su clave privada, cualquier persona que conozca su clave pública podrá descifrar la misma.

En consecuencia, si es posible descifrar un mensaje utilizando la clave pública de una persona, entonces puede afirmarse que el mensaje lo generó esa persona utilizando su clave privada (probando su autoría).

2.4. Certificados Digitales

2.4.1. Definición

Un certificado digital es un archivo electrónico que tiene un tamaño máximo de 2 kilobytes y que contiene los datos de identificación personal del emisor de los mensajes firmados, la clave publica del mismo y la firma privada del propio Prestador de Servicios de Certificación(cuya misión es la de emitir los certificados) con la clave privada de ésta.

Los certificados digitales tienen una duración determinada, transcurrida la cual deben ser renovados, y pueden ser revocados anticipadamente en ciertos supuestos (por ejemplo, en el caso de que la clave privada, que debe permanecer secreta, haya pasado a ser conocida por terceras personas no autorizadas para usarla).

Gracias al certificado digital, el par de claves obtenido por una persona estará siempre vinculado a una determinada identidad personal, y si sabemos que el mensaje ha sido cifrado con la clave privada de esa persona, sabremos también quien es la persona titular de esa clave privada.

2.4.2. Tipos

Las Autoridades de Certificación pueden emitir diferentes tipos de certificados; básicamente son: Certificados de Identidad (personal o digital), Certificados de Autorización (potestad), Certificados Transaccionales (actas y resguardos), y Certificados de Tiempo (estampillado o registro temporal).

- Los Certificados de Identidad son los más utilizados actualmente dentro de los criptosistemas de clave pública y ligan una identidad personal (usuario) o digital (equipo, software, etc.) a una clave pública.
- Los Certificados de Autorización o potestad son aquellos que certifican otro tipo de atributos del usuario distintos a la identidad, como pueden ser, el pertenecer a una determinada asociación, disfrutar de una serie de privilegios, poseer un carnet de conducir, etc.
- Los Certificados Transaccionales son aquellos que atestiguan que algún hecho o formalidad acaeció o fue presenciada por un tercero; el agente de registro al servicio de la Autoridad de Certificación emisora.
- Los Certificados de Tiempo o de estampillado digital de tiempo permiten dar fe de que un documento existía en un instante determinado de tiempo, por lo que constituyen un elemento fundamental de todos los servicios de registro documental y de protección de la propiedad intelectual o industrial que se están proponiendo.

2.4.3. Autoridades de Certificación

La validez de un certificado es la confianza en que la clave pública contenida en el certificado pertenece al usuario indicado en el certificado. La manera en que se puede confiar en el certificado de un usuario con el que no hemos tenido una vinculación anterior es mediante la confianza en terceras partes.

La idea consiste en que dos usuarios puedan confiar entre sí, si ambos tienen relación con una tercera parte la cual podrá dar fé de la fiabilidad de los dos, la cual la constituye la Autoridad Certificante. Una Autoridad Certificante es una tercera parte en la cual otros

confían y que se encarga de establecer la vinculación entre una clave pública y su propietario.

La necesidad de una tercera parte de confianza es fundamental en cualquier entorno de clave pública de tamaño considerable debido a que es improbable que los usuarios hayan tenido relaciones previas antes de intercambiar información cifrada o firmada.

Por otra parte, la mejor manera de permitir la distribución de las claves públicas (o certificados digitales) de los distintos usuarios es que algún agente en quien todos los usuarios confíen se encargue de su publicación en algún repositorio al que todos los usuarios tengan acceso.

La forma en que esta tercera parte avalará que el certificado de un determinado usuario es válido será mediante su firma digital sobre dicho certificado.

En el ejemplo descrito en la Fig. N°2.3 podemos verificar este proceso, Juan envía el mensaje a Mario, lo cual genera dos firmas digitales, la del emisor que firma el correo (la firma de Juan) y la del certificador (autoridad certificante), firmando el certificado de clave pública del emisor (Juan). Del otro lado, el receptor (Mario) obtendrá la clave pública del certificado que fue firmado por el certificador y la podrá utilizar con seguridad en el "proceso de verificación de firma".

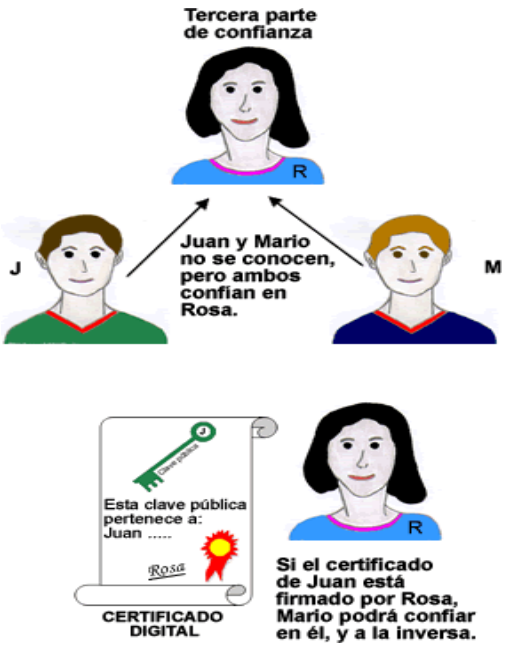


Fig. N° 2.3. Credibilidad en la autoridad Certificadora al momento de comunicarse dos personas.

Jerarquía de Autoridades Certificantes

Se puede inferir que se va formando una cadena de autoridades certificantes. Es de notar que este proceso podría seguirse indefinidamente y no tendría fin, el problema no se resolvería.

Se hace necesario entonces cortar la cadena en algún punto de manera tal que habrá una autoridad certificante de nivel superior a todas las demás, llamada autoridad certificante raíz como se observa en la fig. N° 2.4

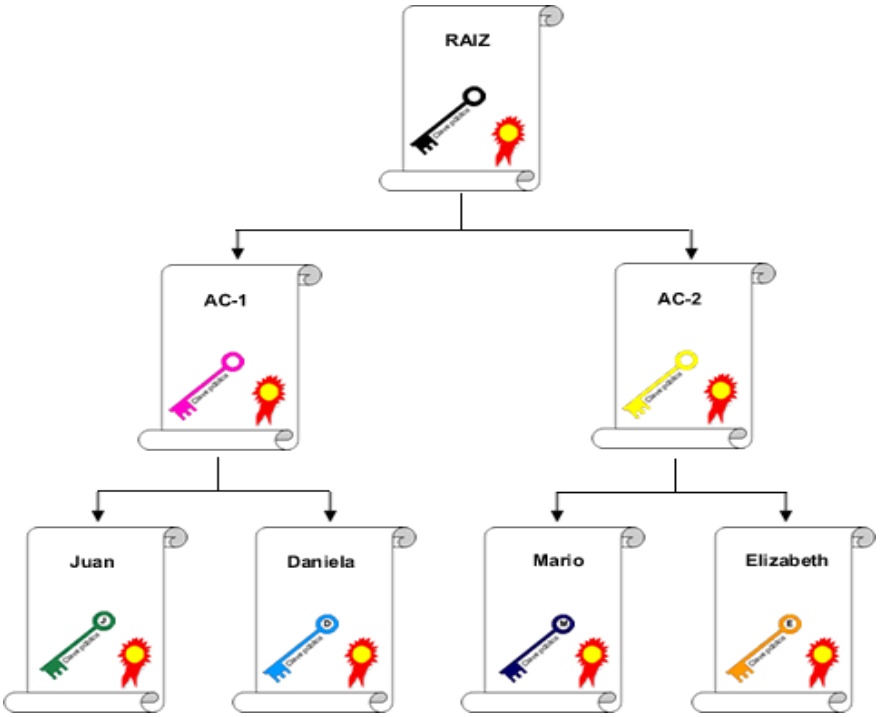


Fig. N° 2.4. Jerarquía de autoridades certificadoras

Esta entidad poseerá un certificado de clave pública auto emitido, es decir, firmado con su propia clave privada, no teniendo validez en si mismo. Será necesario entonces recurrir a algún medio alternativo y seguro que nos permita verificar la clave pública de la autoridad certificante raíz y a partir de allí poder confiar en todos los certificados de clave pública que se encuentren en los niveles inferiores.

2.5. Criptografía

2.5.1. Definición

Es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y es empleada frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

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

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

2.5.2. Tipos de Criptografía

2.5.2.1. Simétrica

2.5.2.1.1. Definición

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

2.5.2.1.2. Inconvenientes

El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad, sino al intercambio de claves. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero ¿qué canal de comunicación que sea seguro han usado para transmitirse las claves? Sería

mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.

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

2.5.2.2. Asimétrica

2.5.2.2.1. Definición

La criptografía asimétrica es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. 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.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la identificación y autenticación del remitente, ya que se sabe que sólo pudo haber sido él quien utilizó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la firma electrónica.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave

pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee

2.5.2.2.2. Seguridad

Como con los sistemas de cifrado simétricos buenos, con un buen sistema de cifrado de clave pública toda la seguridad descansa en la clave y no en el algoritmo. Por lo tanto el tamaño de la clave es una medida de la seguridad del sistema, pero no se puede comparar el tamaño del cifrado simétrico con el del cifrado de clave pública para medir la seguridad. En un ataque de fuerza bruta sobre un cifrado simétrico con una clave de un tamaño de 80 bits, el atacante debe probar hasta 280-1 claves para encontrar la clave correcta. En un ataque de fuerza bruta sobre un cifrado de clave pública con una clave de un tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits (hasta 155 dígitos decimales). La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128 bits son suficientes para cifrados simétricos, dada la tecnología de factorización de hoy en día, se recomienda el uso de claves públicas de 1024 bits para la mayoría de los casos.

2.5.2.2.3. Desventajas del Cifrado Asimétrico

La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene bastantes desventajas:

- Para una misma longitud de clave y mensaje se necesita **mayor tiempo de proceso**.
- Las claves deben ser de mayor tamaño que las simétricas.
- El mensaje cifrado ocupa más espacio que el original.

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

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

2.5.2.2.4. Algoritmos

Algunos algoritmos de técnicas de clave asimétrica son:

- Diffie-Hellman
- RSA
- DSA
- ElGamal
- Criptografía de curva elíptica

Otros algoritmos de clave asimétrica pero inseguros:

- Merkle-Hellman, algoritmos "Knapsack".

CAPITULO III: SEGURIDAD DE LA INFORMACIÓN.

3.1. Definiciones Básicas.

3.1.1. Confidencialidad.

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. Es por ello que las medidas de seguridad deben estar enfocadas a garantizar que la información está disponible para aquellos que estén autorizados a conocerla.

3.1.2. Integridad.

Para la seguridad de la Información, la integridad es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra datos importantes.

3.1.3. Disponibilidad.

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizada para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente.

3.1.4. Otros Conceptos.

- ✓ **Auditabilidad.-** Permitir la reconstrucción, revisión y análisis de la secuencia de eventos
- ✓ **Identificación.-** Verificación de una persona o cosa; reconocimiento.
- ✓ **Autenticación.-** Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, se tiene o una combinación de todas.
- ✓ **Autorización.-** Lo que se permite cuando se ha otorgado acceso
- ✓ **No repudio.-** No se puede negar un evento o una transacción.
- ✓ **Seguridad en capas.-** La defensa a profundidad que contenga la inestabilidad
- ✓ **Control de Acceso.-** Limitar el acceso autorizado solo a entidades autenticadas
- ✓ **Métricas de Seguridad, Monitoreo.-** Medición de actividades de seguridad
- ✓ **Gobierno.-** Proporcionar control y dirección a las actividades
- ✓ **Estrategia.-** Los pasos que se requieren para alcanzar un objetivo
- ✓ **Arquitectura.-** El diseño de la estructura y las relaciones de sus elementos
- ✓ **Gerencia.-** Vigilar las actividades para garantizar que se alcancen los objetivos
- ✓ **Riesgo.-** La explotación de una vulnerabilidad por parte de una amenaza
- ✓ **Exposiciones.-** Áreas que son vulnerables a un impacto por parte de una amenaza
- ✓ **Vulnerabilidades.-** deficiencias que pueden ser explotadas por amenazas
- ✓ **Amenazas.-** Cualquier acción o evento que puede ocasionar consecuencias adversas
- ✓ **Riesgo residual.-** El riesgo que permanece después de que se han implementado contra medidas y controles
- ✓ **Impacto.-** Los resultados y consecuencias de que se materialice un riesgo
- ✓ **Criticidad.-** La importancia que tiene un recurso para el negocio
- ✓ **Sensibilidad.-** El nivel de impacto que tendría una divulgación no autorizada
- ✓ **Análisis de impacto al negocio.-** Evaluar los resultados y las consecuencias de la inestabilidad
- ✓ **Controles.-** Cualquier acción o proceso que se utiliza para mitigar el riesgo

- ✓ **Contra medidas.-** Cualquier acción o proceso que reduce la vulnerabilidad
- ✓ **Políticas.-** Declaración de alto nivel sobre la intención y la dirección de la gerencia
- ✓ **Normas.-** Establecer los límites permisibles de acciones y procesos para cumplir con las políticas
- ✓ **Ataques.-** Tipos y naturaleza de inestabilidad en la seguridad
- ✓ **Clasificación de Datos.-** El proceso de determinar la sensibilidad y Criticidad de la información

3.2. Contraseñas.

Aunque en la actualidad existen varias formas de autenticación de usuarios, la mayoría inician sesión en su equipo y sistemas remotos escribiendo una combinación del nombre de usuario y una contraseña mediante el teclado. Algunos productos emplean tecnologías más seguras como, por ejemplo, la biométrica, las tarjetas inteligentes y las contraseñas de un solo uso para todos los sistemas operativos más habituales. Sin embargo, la mayor parte de las organizaciones siguen confiando en las contraseñas y seguirán haciéndolo en los próximos años. A menudo, los usuarios disponen de varias cuentas de equipo en el trabajo, para el teléfono móvil, el banco, la compañía de seguros, etc. Con el fin de recordar las contraseñas con mayor facilidad, suelen utilizar contraseñas idénticas o parecidas para todas las cuentas. Por otro lado, eligen contraseñas muy sencillas y fáciles de recordar, como su fecha de cumpleaños, el nombre de su madre o el de algún familiar. Las contraseñas cortas y sencillas constituyen un objetivo relativamente fácil para los atacantes.

CAPITULO IV: SEGURIDAD DEL SOFTWARE.

4.1. Análisis de Riesgos.

La información es el activo más importante que se posee hoy en día una empresa, y, por lo tanto, deben existir técnicas y métodos que le den seguridad, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo. Los medios para conseguirlo son:

- ✓ Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
- ✓ Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión).
- ✓ Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
- ✓ Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
- ✓ Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
- ✓ Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
- ✓ Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

4.2. Amenazas.

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguras, todavía deben ser tenidas en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es la redundancia (en el caso de los datos) y la descentralización, por ejemplo mediante estructura de redes (en el caso de las comunicaciones).Estos fenómenos pueden ser causados por:

- **El usuario.-** Causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).
- **Programas maliciosos.-** Programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos, pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.
- **Un intruso.-** Persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, script kiddie o boy, etc.).
- **Un siniestro (robo, incendio, por agua).-** Una mala manipulación o una mal intención derivan a la pérdida del material o de los archivos.

4.3. Técnicas de Aseguramiento del Sistema.

Codificar la información: Criptología, Criptografía y Criptociencia, contraseñas difíciles de averiguar a partir de datos personales del individuo.

Vigilancia de Red.

Tecnologías repelentes o protectoras: Cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc.

Mantener con las actualizaciones: Los sistemas de información con las actualizaciones que más impacten en la seguridad.

4.3.1. Consideraciones de Software.

- Es recomendable tener instalado en la máquina únicamente el software necesario reduce riesgos.
- Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (el software obtenido de forma ilegal o sin garantías aumenta los riesgos).
- En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre.
- El software con métodos de instalación rápidos facilita también la reinstalación en caso de contingencia.

CAPITULO V: AUDITORIA INFORMÁTICA

5.1. Definición.

Es la revisión y evaluación de los controles, sistemas, procedimientos de informática y de los equipos de cómputo, su utilización, eficiencia y seguridad, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría informática debe partir de una situación dada; ésta es metódica, puesto que seguirá un plan de trabajo perfectamente sistematizado que permite llegar a conclusiones suficientemente justificadas; es puntual ya que se da un corte en el calendario para llevarla a cabo, y es extraña al servicio de informática, para obtener la objetividad requerida, por lo que será ejecutada por personas ajenas al departamento independientes de las funciones a auditar.

5.2. Tipos de Auditoria Informática

Auditoría Informática de Explotación.- Auditar Explotación consiste en evaluar los datos, su transformación, los controles de integridad y calidad, y sus interrelaciones.

Auditoría Informática de Desarrollo de Proyectos o Aplicaciones.- Consiste en auditar aplicaciones en desarrollo, en sus diferentes fases, puesto que deben estar sometidas a un exigente control interno; caso contrario, además del disparo de los costes, podrá producirse la insatisfacción del usuario. Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la máquina sean exactamente los previstos y no otros.

Auditoría Informática de Sistemas.- Es el examen o revisión de carácter objetivo (independiente), crítico(evidencia), sistemático (normas), selectivo (muestras) de las políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con los sistemas de información computarizados, con el fin de emitir una opinión profesional (imparcial) con respecto a: eficiencia en el uso de los recursos informáticos, validez de la información y efectividad de los controles establecidos.

Auditoría de la Seguridad Informática.- Abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotaje, robos, catástrofes naturales, etc. La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

5.3. Proceso Metodológico para elaborar una Auditoría Informática

5.3.1. Diagnóstico.

Esta fase incluye a la alta dirección y las áreas usuarias. Se busca la opinión de la primera para saber el grado de satisfacción y confianza que tienen en los productos, servicios y recursos de informática en el negocio. Se detectan las fortalezas, aciertos, apoyo que brinda dicha función y las oportunidades que puede ofrecer la informática para hacer más competitivo el negocio.

Conocimiento del negocio.- El auditor en informática debe conocer: la misión, estrategias, planes, el nivel jerárquico de la función de informática y las entidades externas a la empresa que se relacionan con cada área de la misma.

Apoyo al negocio.- El auditor informático debe tener una idea global del grado de apoyo y satisfacción que existe en el negocio, y saber hacia dónde se orienta el soporte de la función de informática.

Áreas de oportunidad.- Se detectan las características que van a facilitar la implementación de soluciones brindadas por informática y que tendrán gran impacto sobre alguna función del negocio. Las áreas de oportunidad deben ser analizadas y documentadas antes de ponerlas en práctica.

Diagnóstico de informática.- Aquí el auditor se coordina directamente con el responsable de la función de informática.

Conocimiento de la función de informática.- El auditor conocerá la estructura interna de informática, funciones, objetivos, estrategias, planes y políticas, para lo que se apoyará en la tecnología de software y hardware.

5.3.2. Etapa de Justificación.

El auditor se centrará en elaborar un documento fundamental para la aprobación del proyecto, el mismo que debe contemplar: las áreas que se auditarán (matriz de riesgo), el tiempo sugerido para hacerlo (plan de auditoría informática) y el visto bueno (compromiso ejecutivo).

Matriz de riesgo.- El objetivo principal es detectar las áreas de mayor peligro en relación con informática y que requieren una revisión formal y oportuna y determinar el nivel de riesgo que existe en cada área detectada, para asegurar que se desarrolle de acuerdo con los estándares, políticas y procedimientos que se le asignaron según su función.

Plan de auditoría informática.- Consiste en plantear las tareas más importantes que se ejecutarán durante cierto período al efectuar la auditoría. Este plan se deriva de los siguientes elementos: Áreas de oportunidad, matriz de riesgos y las prioridades de la alta dirección, de auditoría y de informática.

Compromiso ejecutivo.- Su objetivo principal es obtener el visto bueno inicial de la alta dirección y demás responsables para continuar con el proyecto de auditoría.

5.3.3. Etapa de Adecuación.

Esta etapa es un conjunto de tareas estructuradas para que el proyecto de auditoría informática se adapte a las necesidades de la empresa estudiada, pero sin olvidar la referencia de los estándares, políticas y procedimientos de auditoría que siempre son aceptados y recomendados por las asociaciones relacionadas con el proceso. Los elementos que se deben contemplar son:

Objetivos y requerimientos de éxito por cada área que se auditará.- Se desarrolla tomando como base la matriz de riesgo. Debido a que a medida que avanza el proyecto, surgen cancelaciones, prioridades, requerimientos, expectativas, nuevos involucrados, etc., el auditor debe actualizar el plan de trabajo, detallar fechas, tiempos, resultados esperados, responsabilidades y funciones, así como estimar gastos y el número de personas que participarán.

Plan detallado del proyecto de auditoría informática.- Se define cada detalle de los elementos del proyecto; se especifican las tareas, productos terminados, responsables, fechas, etc., que serán validados y aprobados en la etapa de formalización para arrancar el proyecto. Hay dos tipos de planes detallados:

- Plan interno, que le corresponde al líder de proyecto y su propósito es hacer un seguimiento interno a las tareas y responsabilidades de los auditores.
- Plan detallado de auditoría en informática, en el que se especifica el detalle emanado del plan general de auditoría informática.

Definición de técnicas y herramientas.- Consiste en definir las técnicas y herramientas esenciales para revisar eficientemente cada área seleccionada.

Adecuación a la alta política de empresa.- Todas las tareas realizadas por la auditoría informática deben cumplir con los estándares, políticas y procedimientos establecidos por asociaciones profesionales y por las empresas donde se preste el servicio.

Elaboración de cuestionarios.- Se estructuran de manera que sirven de guía para verificar la confiabilidad de la información del personal entrevistado; además, permiten percibir el grado de cumplimiento de estándares, políticas y procedimientos que generalmente son aceptados.

5.3.4. Etapa de Formalización.

En esta etapa la alta dirección da su aprobación y apoyo formal para el desarrollo del proyecto de auditoría, de tal manera que, su función es justificar el desarrollo del proyecto basándose en lo que se hizo en las etapas anteriores.

Verificación de prioridades, restricciones y alcance del proyecto.- Permite la clarificación del rumbo, límites y cobertura que tendrá el proyecto.

Presentación formal del plan de auditoría informática.- Se justificará la continuidad del proceso, para lo cual el responsable de esta tarea deberá:

- Asegurarse de contar con toda la información resumida y presentable.
- Revisarla y verificarla.
- Concertar en una cita en una fecha y lugar apropiados.
- Ser fluido, claro y contundente en la presentación.

- Asegurar el entendimiento de la audiencia de los datos presentados.

Aprobación formal del proyecto.- En esta tarea surge la aprobación formal del proyecto de auditoría.

Compromiso ejecutivo.- Lograr que la alta dirección, los usuarios clave, el responsable de informática y el de la auditoría se comprometan a lo largo del proyecto, desde ese momento hasta el desarrollo e implantación de las acciones recomendadas por auditoría informática en su informe final.

5.3.5. Etapa de Desarrollo.

El auditor informático comienza a ejecutar sus tareas de acuerdo con el plan aprobado en la etapa anterior. Esta fase comprende:

- ✓ Concertación de fechas de entrevistas, visitas y de aplicación de cuestionarios.
- ✓ Verificación de las tareas, involucrados y productos terminados.
- ✓ Clasificar técnicas y herramientas.
- ✓ Aplicación de entrevistas y cuestionarios.
- ✓ Efectuar visitas para la verificación.
- ✓ Elaboración de informes preliminares.
- ✓ Revisión de estos informes.
- ✓ Clasificación y documentación de los informes, para su correcta lectura.
- ✓ Finalización de tareas o productos pendientes.
- ✓ Elaboración del informe final de la auditoría informática.
- ✓ Presentación a la alta dirección e involucrados clave.
- ✓ Aprobación del proyecto y compromiso ejecutivo.

5.3.6. Etapa de Implantación

En ésta fase los responsables de las áreas usuarias y de informática ejecutarán las acciones recomendadas en los informes detallados y aprobados por la alta dirección. La función del auditor se convierte así en una labor de seguimiento y apoyo. Los elementos clave de la etapa de implantación son:

- Definición de requerimientos para el éxito de la etapa de implantación.
- Desarrollo del plan de implantación.
- Implantación de las acciones sugeridas por auditoría en informática.
- Seguimiento a la implantación

5.4. Auditoria de Sistemas.

5.4.1. Objetivos Específicos.

- ✓ Evaluación de la seguridad en el área informática.
- ✓ Evaluación de suficiencia en los planes de contingencia: respaldos, prevención de acontecimientos.
- ✓ Opinión de la utilización de los recursos informáticos: resguardo y protección de activos.
- ✓ Control de modificación a las aplicaciones existentes: fraudes, control a las modificaciones de los programas.
- ✓ Participación en la negociación de contratos con los proveedores.
- ✓ Revisión y control de la utilización del sistema operativo y los programas: utilitarios.
- ✓ Auditoría de la base de datos.: estructura sobre la cual se desarrollan las aplicaciones.
- ✓ Auditoría de la red de teleprocesos.
- ✓ El Análisis y control de la función informática (Sistema de Información - SI y la Tecnología de la Información -TI).
- ✓ La verificación del cumplimiento de la Normativa General de la Organización.
- ✓ La verificación de los Planes, Programas y Presupuestos de los Sistemas Informáticos.
- ✓ La revisión de la eficaz gestión de los recursos materiales y humanos informáticos.
- ✓ La revisión y verificación de las Seguridades: Cumplimiento de normas y estándares, Sistema Operativo, Seguridad de Software, Seguridad de Comunicaciones, Seguridad de Base de Datos, Seguridad de Proceso, Seguridad de Aplicaciones, Seguridad Física, Suministros y Reposiciones, Contingencias.
- ✓ El análisis del control de resultados.
- ✓ El análisis de verificación y de exposición de debilidades y disfunciones.

5.4.2. Fines de la Auditoria de Sistemas.

- Fundamentar la opinión del auditor interno (externo) sobre la confiabilidad de los sistemas de información.
- Expresar la opinión sobre la eficiencia de las operaciones en el área de TI.

5.4.3. Herramientas y Técnicas para la Auditoría de Sistemas.

- ✓ Cuestionarios.
- ✓ Entrevistas.
- ✓ Formularios Checklist.
- ✓ Formularios Virtuales.
- ✓ Pruebas de Consistencias.
- ✓ Inventarios y Valorizaciones.
- ✓ Historias de cambios y mejoras.
- ✓ Reporte de Bases de Datos y Archivos
- ✓ Reportes de Estándares.
- ✓ Compatibilidades e Uniformidades.
- ✓ Software de Interrogación:
- ✓ Certificados, Garantías, otros del Software.
- ✓ Fotografías o Tomas de Valor (Imágenes).
- ✓ Diseño de Flujos y de la red de Información.
- ✓ Planos de Distribución e Instalación (Para Estudio y Revisión).
- ✓ Listado de Proveedores, entre otros.

CAPITULO VI: ILUSTRE MUNICIPIO DE CALVAS

6.1. Historia.

Calvas, en la época precolombina constituyó la nación indígena Curimanga y luego en la colonia la provincia de Calvas, la misma que comprendía los territorios de los actuales cantones: Macara, Calvas y parte de Gonzanamá, en la época de la Gran Colombia, el antiguo pueblo y asiento de Cariamanga fué elevado a la categoría de villa y cabecera cantonal.

El 25 de junio de 1824, El Excelentísimo Vicepresidente de la Gran Colombia, encargado del poder ejecutivo, Francisco de Paula Santander, impone el ejecútese, al decreto promulgado por la Cámara y El Senado reunidos en congreso, mediante el cual se establece la división territorial de la Gran Colombia. Y en el párrafo segundo del artículo 12 del mencionado decreto se crea el Cantón Cariamanga como parte de la jurisdicción de la Provincia de Loja.

En aquel entonces, el Cantón Cariamanga comprendía los territorios del actual cantón Calvas, de los de Macará y parte de los de Gonzanamá, y estaba formado por las parroquias: Cariamanga, Sozoranga, Macará y Amaluza, siendo Cariamanga la Cabecera Cantonal del Cantón Cariamanga. (hoy Calvas).

En 1830 El Gobierno de la República del Ecuador ratifica la creación del cantón Cariamanga, hecha en época de La Gran Colombia en 1824. El Gobierno Federal de Loja, en octubre de 1859, decreta la división territorial y política de La Provincia de Loja en cinco cantones, siendo uno de ellos el de Calvas.

El cantón Calvas fué creado el 14 de Octubre de 1863, en la Presidencia del Dr. Gabriel García Moreno.

6.2. Estructura.

Actualmente el Gobierno Seccional del cantón Calvas de encuentra integrado por la siguiente mesa directiva:

1. Dr. Franklin Cueva Rosillo. ALCALDE DEL CANTON
2. Dr. Mario Cueva Bravo. VICEPRESIDENTE DEL MUNICIPIO

3. Prof. Carmelita Quezada CONCEJAL
4. Ing. Marco Alonso Torres CONCEJAL
5. Arq. César Jiménez Jiménez CONCEJAL
6. Lic. Luis Castillo CONCEJAL
7. Sr. Alex Padilla CONCEJAL
8. Lic. Manuel Ruiz CONCEJAL

CUADRO DE COMISIONES PERMANENTES GENERALES

Comisión de mesa, excusas y calificaciones

- Dr. Franklin Cueva Rosillo PRESIDENTE.
- Dr. Mario Cueva Bravo PRIMER VOCAL.
- Prof. Carmelita Quezada SEGUNDO VOCAL

Comisión de planeamiento, urbanismo y obras públicas.

- Ing. Marco Alonso Torres. PRESIDENTE
- Lic. Luis Castillo PRIMER VOCAL
- Prof. Carmelita Quezada SEGUNDO VOCAL

Comisión de servicios públicos que comprende: abastecimiento de agua, alcantarillado, y aseo público, bomberos, mataderos, plazas de mercado, cementerios y otros que pueden calificarse como tales.

Comisión de agua potable y alcantarillado

- Dr. Mario Cueva Bravo PRESIDENTE
- Sr. Alex Padilla Torres. PRIMER VOCAL
- Prof. Carmelita Quezada SEGUNDO VOCAL

Comisión de servicio financiero que incluye: presupuesto, impuestos, tasas y contribuciones, deuda pública, suministro y enseres municipales.

- Prof. Carmelita Quezada PRESIDENTE
- Lic. Luis Castillo PRIMER VOCAL
- Ing. Marco Alonso Torres SEGUNDO VOCAL

Comisión deservicios sociales que abarca: higiene, salubridad y servicios asistenciales, educación y cultura

- Lic. Luis Castillo PRESIDENTE
- Arq. César Jiménez PRIMER VOCAL
- Prof. Carmelita Quezada SEGUNDO VOCAL

Comisión de servicios económicos, como vías de comunicación, transporte, almacenaje, control de precios, servicios de telecomunicaciones, agricultura, industria y otros de naturaleza semejante.

- Ing. Marco Alonso Torres PRESIDENTE
- Lic. Luis Castillo PRIMER VOCAL
- Lic. Manuel Ruíz SEGUNDO VOCAL

6.3. Servicios.

Ciertos recursos materiales humanos y económicos del Cantón, son administrados por un organismo denominado concejo municipal. El concejo municipal está conformado por el ALCALDE y CONCEJALES, los mismos que son elegidos por el pueblo mayor de edad de la jurisdicción cantonal de las listas de candidatos presentados por los denominados “Partidos Políticos”. El Cantón Calvas tiene 1 alcalde y 7 concejales. El Alcalde es la persona que ejecuta las decisiones tomadas por el Consejo Municipal; dura 4 años en su función. Los Concejales conjuntamente con el alcalde toman las decisiones, Sesionan en forma ordinaria una vez por semana. El Municipio se encarga de:

- ✓ Regula el crecimiento urbanístico dentro de la jurisdicción.
- ✓ Dotar de agua potable a sus habitantes.
- ✓ Construir servicio de alcantarillado para conducir las aguas servidas.
- ✓ Mantener limpios los centros poblados.
- ✓ Dotar de sitios de recreación a sus habitantes.
- ✓ Construir mercados.
- ✓ Ayudar al mejoramiento de la calidad de educación
- ✓ Controlar que el medio ambiente no sea contaminado por sus habitantes.
- ✓ Otras acciones que de acuerdo a la descentralización les asignen.

6. METODOLOGÍA

6.1. MATERIALES, MÉTODOS Y TÉCNICAS DE TRABAJO

El desarrollo de nuestro proyecto de tesis se fundamenta en la utilización de métodos, metodologías, técnicas e instrumentos encargados de facilitar la recolección de la información, de manera que la problemática definida anteriormente pueda ser resuelta y podamos así cumplir con los objetivos ya establecidos.

MÉTODOS

- **Método Deductivo.**

El cual se caracteriza principalmente por partir de datos generales aceptados como válidos para llegar a una conclusión de tipo particular.

En nuestro caso para la construcción del Sistema Automatizado de Gestión de Documentos utilizando certificados digitales, hemos creído conveniente utilizar este método, ya que nos permitió determinar cuáles son los inconvenientes que se suscitan actualmente al momento de tramitar información de un departamento a otro, es decir durante el envió o recepción de datos. Algunos de los inconvenientes más relevantes encontrados hasta el momento son: Retrasos en la entrega de información, pérdida de documentos, uso prolongado de tiempo para la aceptación de algún tipo de contrato, accesos no autorizados a la información confidencial, posibilidad de que exista conocimiento del contenido de los mensajes o información tramitada entre un departamento y otro por parte de personal no autorizado, entre otros , llegando por lo tanto a la conclusión de que la resolución de éste tipo de tareas es un proceso tedioso y que requiere que sea controlado debidamente en base a los estándares de seguridad y confidencialidad de información existentes tales como el "uso de firmas digitales", tomando en cuenta que se encuentren bajo tutela de entidades certificadoras para tales efectos.

- **Método Inductivo.**

Se fundamenta en partir de los datos particulares para llegar a conclusiones generales. Es por ello que en base al análisis y clasificación de la información éste método nos facilitó el encontrar que la solución a los inconvenientes que se presentan actualmente en los departamentos municipales es el "***"****Diseño y construcción de un sistema automatizado para la gestión de documentos en la Ilustre Municipalidad del cantón Calvas utilizando*

certificados digitales"", el cual será un aporte significativo, debido a que facilitará la resolución de tareas en el cada uno de los departamentos involucrados en la tramitación de documentos, beneficiando por tanto no solo a dicha institución sino también a la ciudadanía en general brindando un servicio más óptimo y eficiente.

☞ **Ciclo de Vida Clásico para el Desarrollo de Software**, Mediante el cumplimiento de etapas ordenadas nos permitirá obtener un producto de calidad fundamentado en las necesidades que existen y se verifican actualmente en el Ilustre Municipalidad del cantón Calvas. Las fases que se definen dentro de ésta metodología son:

✓ **Análisis y determinación de los requerimientos del sistema.-** En esta etapa se recolectará toda la información referente a los procesos que se efectúan al momento de tramitar algún tipo de documento considerando para ello el nivel de relación o vinculación entre un departamento y otro, hecho que se da actualmente en el Municipio de Calvas, para ello utilizaremos algunas técnicas de recolección de datos tales como entrevistas y observación directa, con la finalidad de identificar las características que tendrá el nuevo sistema, incluyendo la información que el sistema debe producir y las características operativas, como son controles de procesamiento, tiempos de respuesta y métodos de entrada y salida.

✓ **Diseño de la aplicación.-** En esta fase se pretende definir los detalles que establecen la forma en la que el sistema cumplirá con los requerimientos identificados durante la fase de análisis. Para ello se hará uso de algunas de las herramientas automatizadas disponibles para el diseño de sistemas como la metodología ICONIX la cual nos permitirá construir un prototipo que se espera que aparezca cuando el sistema está terminado, también se indican los procedimientos a seguir para los datos de entrada, almacenamiento y salida que tendrá el sistema. La información detallada en el diseño nos permitirá comenzar la fase de desarrollo de software.

✓ **Desarrollo del sistema.-** Aquí desarrollaremos los diferentes módulos que conformaran el sistema de Gestión de Documentos y que hayan sido especificados en la etapa anterior. Utilizaremos las diferentes herramientas de desarrollo disponibles en el mercado de manera que nos lleven a construir un software de calidad. En esta etapa también se creara toda la documentación necesaria para explicar, probar el programa y hacer el mantenimiento.

✓ **Pruebas y corrección.-** Durante todo el desarrollo del software se realizaran pruebas al software de acuerdo a la funcionalidad de que éste presente hasta un momento dado. Así mismo el sistema se empleará de manera experimental para asegurarnos que no tenga fallas, es decir, que funcionará de acuerdo con las especificaciones y en la forma en que los usuarios esperan que lo haga. Se empleará datos reales para dichas pruebas y después se examinarán los resultados.

✓ **Implantación.-** Etapa que consistirá en verificar el equipo(hardware) en base a las especificaciones ya definidas e instalar el sistema Automatizado para la Gestión de Documentos, entrenar a los usuarios, y construir todos los archivos de datos necesarios para utilizarla. Cabe recalcar que esta etapa será considerada, solo si la institución autoriza la implementación de la aplicación a desarrollar.

METODOLOGÍA PARA EL DESARROLLO DE LA APLICACIÓN

☞ **ICONIX**, Caracterizada principalmente por manejar casos de uso. Es relativamente pequeño y firme, no desecha el análisis y diseño, haciendo uso aerodinámico del UML mientras guarda un enfoque afilado en el seguimiento de requisitos. Es flexible para diferentes estilos y clases de problemas, por ello, esta metodología está definida como un Proceso de Desenvolvimiento desarrollado para Ingeniería de Software. Su enfoque es el siguiente:

- ✓ Modelado de objetos conducido por casos de uso
- ✓ Centrado en datos: se descompone en fronteras de datos
- ✓ Basado en escenarios que descomponen los casos de uso
- ✓ Enfoque iterativo e incremental
- ✓ Ofrece trazabilidad
- ✓ Uso directo de UML.

Los pasos a seguir para aplicar ésta metodología son los siguientes:

✓ Análisis de requerimientos:
META: Revisión de requerimientos.

- Identificar objetos del dominio y relaciones de agregación y generalización.
- Prototipo rápido.
- Identificar casos de uso.

- Organizar casos de uso en paquetes.
- Asignar requerimientos funcionales a casos de uso y objetos del dominio.

✓ Análisis y diseño preliminar:

META: Revisión del diseño preliminar.

- Escribir descripciones de casos de uso.
  - ❖ cursos normales y alternos
- Análisis de robustez.
  - ❖ Identificar grupos de objetos que realizan escenario.
  - ❖ Actualizar diagramas de clases del dominio.
- Finalizar diagramas de clases.

✓ Diseño:

META: Revisión crítica del diseño

- Asignar comportamiento.
- Para cada caso de uso.
  - ❖ Identificar mensajes y métodos.
  - ❖ Dibujar diagramas de secuencia.
  - ❖ Actualizar clases.
- Terminar modelo estático.
- Verificar cumplimiento de requerimientos.

✓ Implantación:

META: Entrega del sistema

- Producir diagramas necesarios.
  - ❖ Despliegue.
  - ❖ Componentes.
- Escribir el código.
- Pruebas de unidad e integración.
- Pruebas de sistema y aceptación basadas en casos de uso.

6.2. TÉCNICAS

- **Entrevista** que será realizada a los encargados de cada departamento del Ilustre Municipio del cantón Calvas, para obtener la información necesaria acerca del funcionamiento de los diferentes procesos que se efectúan en el momento de tramitar algún tipo de documento ya sea durante su envió como en su recepción.

- **Observación directa** de los procesos desarrollados en los departamentos involucrados en la gestión de documentos de diversa índole que se efectúan en el Municipio de Calvas, con la finalidad de tener una visión clara de la realidad existente dentro de esta institución; y así poder identificar los inconvenientes más significativos en el cumplimiento de sus actividades.
- **Lectura Científica** misma que la utilizaremos para investigar todos los referentes teóricos sobre seguridad, confidencialidad, firmas digitales y demás temas que nos faciliten la sustentación del desarrollo del presente proyecto de tesis.

6.3. INSTRUMENTOS

- Fuentes bibliográficas e Internet, que nos permitirán recopilar la información necesaria acerca de: Municipio de Calvas,Firmas Digitales, Seguridad de la Información, Seguridad del Software, Tecnologías para la Seguridad de la Información; todos ellos enfocados al desarrollo del presente proyecto de tesis.

- Hardware y software que apoyarán a la elaboración tanto de la documentación, como del desarrollo de la aplicación.
  - ☞ Dos ordenadores, cuyas características técnicas serán detalladas en la sección de Recursos del presente informe.
  - ☞ Equipos de Impresión.
  - ☞ Enterprise Architect 4.10
  - ☞ Sistema Operativo: Windows XP
  - ☞ Herramienta para la Planificación: Microsoft Office Project 2003.
  - ☞ Herramienta para la edición: Paquete de Microsoft Office 2007.
  - ☞ Lenguaje de Programación: JAVA Plataforma 2 v1.6.0 o superior
  - ☞ Herramienta para diseño y codificación: Eclipse v3.3.0
  - ☞ Software de gestión de Bases de Datos: Mysql v 5.0.9.

7. CRONOGRAMA

7. PRESUPUESTO Y FINANCIAMIENTO

8.1. RECURSOS HUMANOS

RECURSOS HUMANOS			
Desarrolladores			
Nombres	**Valor por hora**	**Nº de horas**	**Valor Total**
Patricia Chamba	0.00	2528	$ 0.00
Franklin Andrade	0.00	2528	$ 0.00
Asesores			
Ing. Pablo Costa	0.00	5	0.00
Dra. Nora Tene	0.00	120	0.00
SUBTOTAL			$ 0.00

8.2. RECURSOS MATERIALES

RECURSOS MATERIALES			
Material	**Cantidad**	**Unidad**	**Valor Total**
Anillado	10	$ 1,0	$ 10,00
Empastado	5	$ 5,0	$ 25,0
Carpetas de perfil	10	$ 0,45	$ 4,50
CD-R	25	$ 0,35	$ 8,75
Copias	2000	$ 0,02	$ 40,00
Grapadora	1	$ 3,00	$ 3,00
Grapas	2	$ 0,50	$ 1,00
Perforadora	1	$ 4,00	$ 4,00
Portaminas	2	$ 0,70	$ 1,40
Resma de Papel Inen A4	10	$ 4,50	$ 45,00
Tinta negra	10	$ 2,70	$ 27,00
Tinta de color	5	$ 3,50	$ 17,50
Infocus	4	$ 10,00	$ 40,00
SUBTOTAL			$ 227,15

8.3. SERVICIOS BÁSICOS

SERVICIOS BÁSICOS	
Servicio	**Valor Total**
Luz	$ 100,00
Teléfono	$ 100,00
Transporte	$ 200,00
SUBTOTAL	$ 400,00

8.4. RECURSOS TÉCNICOS Y TECNOLÓGICOS

HARDWARE					
Equipo	**Cantidad**	**Costo**	**Días**	**Depreciación**	**Valor Total**
Computadora de escritorio	1	$ 1000,00	316	$ 365,69	$ 634,31
Computadora de escritorio	1	$ 800,00	316	$ 232,71	$ 576,29
Flash Memory	2	$ 18,00	316	$ 1,85	$ 3,60
Impresoras	2	$ 50,00	316	$ 13.29	$ 26.58
SUBTOTAL					$ 1240,78

SOFTWARE	
Aplicación	**Valor Total**
Enterprise Architect 4.0.0	$25,00
Lenguaje de Programación : JAVA Plataforma 2 v1.6	$3,00
Entorno de Desarrollo: Eclipse v3.3	$3,00
Software de gestión de Bases de Datos: Mysql v 5.0.9.	$3,00
Herramienta para administración de Bases de Datos: Xammp v1.6.8	$3,00
SO: Windows XP Professional	$ 168,23
Herramienta para la edición: Paquete de Microsoft Office 2007	$275 ,00
SUBTOTAL	$480,23

COMUNICACIONES	
Medio	**Valor Total**
Internet	$ 80,00
SUBTOTAL	$ 80,00

RECURSOS TÉCNICOS Y TECNOLÓGICOS	
Recurso	**Valor Total**
Hardware	$ 1240,78
Software	$ 480,23
Comunicaciones	$ 80,00
SUBTOTAL	$ 1801,01

8.1. RESUMEN DE COSTOS

RESUMEN DE COSTOS	
Recurso	**Total**
Recursos Humanos	$ 0.00
Recursos Materiales	$ 227,15
Servicios Básicos	$ 400,00
Recursos Técnicos y Tecnológicos	$ 1801,01
SUBTOTAL	$ 2.428,16
IMPREVISTOS (5%)	$121,41
TOTAL	$2.549,57

9. BIBLIOGRAFÍA

Enlaces web

- ✓ BANCO CENTRAL DEL ECUADOR [en linea] Disponible en [http://www.bce.fin.ec/files.php?file=./documentos/ElBancoCentral/EntidadCert/indice.htm] [Consulta: 17 Febrero 2009]
- ✓ LLULL, Eduard. 2001 Criptografía - Firmas digitales ilustradas [en linea] Disponible en [http://bulma.net/body.phtml?nIdNoticia=868] España [Consulta: 15 Enero 2009]
- ✓ LABORERO, Diego , 2008 Firma Digital [en línea] Disponible en [http://cxo-community.com.ar/index.php?option=com_content&task=view&id=1281&Itemid=1&utm_source=emBlue_Boletin$16&utm_medium=Oferta:617407]Sevilla [Consulta: 07 Febrero 2009]
- ✓ SAVOLAINEN, Martti, 2004 Métodos de Encriptación [en linea] Disponible en [http://www.cibernarium.tamk.fi/seguridad_2/salausmenetelmat.htm]Mexico[Consulta: 22 Enero 2009]
- ✓ VEGA Lebrún GUTIÉRREZ , Arvizu y GARCÍA Santillán**,** 2008 *Algoritmos para encriptación de datos*, < riqueza, la de producción práctico>Edición electrónica gratuita [en linea] Disponible en [http: //www.eumed.net/libros/2008a/348/]Colombia[Consulta: 20 Enero 2009]
- ✓ RAMON, Santiago, 2005 Funciones Hash [en linea] Disponible en [http://foro.elhacker.net/criptografia/funciones_de_hash-t100025.0.html] Mèxico[Consulta: 30 Enero 2009]
- ✓ Wikipedia, 2010 MD5 [en línea] Disponible en [http://es.wikipedia.org/wiki/MD5][Consulta: 10 de Enero del 2009]
- ✓ Wikipedia, 2010 Secure Hash Algorithm [en línea] Disponible en: [http://es.wikipedia.org/wiki/Secure_Hash_Algorithm] [Consulta: 10 de Enero del 2009]
- ✓ Wikipedia, 2010 Seguridad de la información [en línea] Disponible en [http://es.wikipedia.org/wiki/Seguridad_de_la_información] [Consulta: 15 de Enero del 2009]

- ✓ FARIAS, Mariela , 2003 Firma digital [en linea] Argentina Disponible en [http://www.monografias.com/trabajos42/firmas-digitales/firmas-digitales.shtml][Consulta: 17 Enero 2009]
- ✓ MACKAY, Patrick, 2004 Encriptación Asimétrica [en linea] Disponible en [http://msmvps.com/blogs/pmackay/archive/2004/11/27/easim1.aspx] Argentina[Consulta: 04 Febrero 2009]
- ✓ NAVARRO , X, 2000 ¿Qué es un certificado digital? [en linea] Disponible en [http://www.poliedric.com/docs/certdigital.php]Barcelona [Consulta: 04 Febrero 2009]
- ✓ SANTOS, Sergio. Seguridad – Firma digital [en linea] [en linea] Disponible en [http: //portalmundos.com/mundoinformatica/internet/firmadigital.html] España [Consulta: 15 Enero 2009]

10. ANEXOS

MATRIZ DE CONSISTENCIA GENERAL

PROBLEMÁ GENERAL DE INVESTIGACION: “La falta de un sistema automatizado que disponga de niveles de seguridad que garanticen la gestión de documentos tanto en su recepción como en su envió en la Ilustre Municipalidad del cantón Calvas, ocasiona que se brinde un servicio de baja calidad e inseguro durante la tramitación de documentos en esta institución”			
TEMA	**OBJETO DE INVESTIGACIÓN**	**OBJETIVO GENERAL**	**HIPÓTESIS**
“Diseño y construcción de un sistema automatizado para la gestión de documentos en la Ilustre Municipalidad del cantón Calvas utilizando certificados digitales”.	Documentación tramitada: Actas de sesiones, ordenanzas, resoluciones, convenios, órdenes de pago, solicitudes de los departamentos, boletines de prensa, oficios recibidos y enviados, procesos de contratación (contrataciones, licitaciones, calificaciones), y contratos de obras ejecutadas, leyes y registros oficiales.	“Diseñar y construir un sistema automatizado para la gestión de documentos en la Ilustre Municipalidad del cantón Calvas utilizando certificados digitales”	El diseño y construcción de un sistema automatizado para la gestión de documentos en la Ilustre Municipalidad del cantón Calvas utilizando certificados digitales, permitirá garantizar la seguridad e integridad de los diferentes documentos que se tramitan en esta institución, de manera tal que puedan llegar a su destino de manera completa y sin alteraciones.

MATRIZ DE CONSISTENCIA ESPECÍFICA→ 1

PROBLEMA ESPECÍFICO.- Desorganización de la información existente en cada uno de los departamentos pertenecientes al Municipio del cantón Calvas.			
OBJETIVO ESPECÍFICO	**HIPÓTESIS ESPECÍFICA**	**UNIDAD DE OBSERVACIÓN**	**SISTEMA CATEGORIAL**
✓ Organizar los documentos de acuerdo a su índole de manera que se garantice eficiencia y eficacia durante su acceso.	• La organización de la documentación que se tramita en el Municipio de Calvas permitirá que su acceso se lleve a cabo de manera fácil y oportuna, evitando así que se produzca cualquier tipo de retraso.	• Sistemas de gestión de documentos. • Ilustre Municipalidad del cantón Calvas.	• Acceso a los documentos. • Organización de los documentos. • Enfoques generales para la organización de documentos. • Estructura y Políticas del Municipio de Calvas.

MATRIZ DE CONSISTENCIA ESPECÍFICA→ 2

PROBLEMA ESPECÍFICO.- Inexistencia de certificados digitales encargados de asegurar la integridad de los documentos que se tramitan en los diferentes departamentos del Municipio de Calvas.			
OBJETIVO ESPECÍFICO	**HIPÓTESIS ESPECÍFICA**	**UNIDAD DE OBSERVACIÓN**	**SISTEMA CATEGORIAL**
✓ Generar certificados de autenticación que permitan firmar digitalmente la información que se enviará y recibirá entre los diferentes departamentos que conforman la institución	• La utilización de certificados digitales durante la tramitación de documentos garantizará seguridad y autentificación en el contenido de dicha información.	• Firma digital.	• Claves privadas y públicas. • Certificados digitales. • Definición, tipos y autoridades de certificación.

MATRIZ DE CONSISTENCIA ESPECÍFICA→ 3

PROBLEMA ESPECÍFICO.- Falta de seguridad durante el acceso al contenido de los documentos en estado de tramitación o que ya han sido tramitados.			
OBJETIVO ESPECIFICO	**HIPÓTESIS ESPECÍFICA**	**UNIDAD DE OBSERVACIÓN**	**SISTEMA CATEGORIAL**
✓ Usar funciones hash para generar datos asociados (huella digital) basados en la encriptación asimétrica o codificación de los documentos digitales.	• El proceso de encriptación asimétrica, garantizará confidencialidad y autenticidad en el envío y recepción de la información, evitando con ello que personas no autorizadas tengan accesos a su contenido.	• Seguridad de la información • Firma digital.	• Confidencialidad, integridad y disponibilidad. • Funcionamiento de una firma digital. • Criptografía. • Criptografía asimétrica. • Algoritmos de encriptación. • Estándares principales de criptografía.

MATRIZ DE CONSISTENCIA ESPECÍFICA→ 4

PROBLEMA ESPECÍFICO.- Falta de utilización de claves públicas y privadas emitidas por entidades de certificación, en las huellas digitales que hayan sido obtenidas.			
OBJETIVO ESPECIFICO	**HIPÓTESIS ESPECÍFICO**	**UNIDAD DE OBSERVACIÓN**	**SISTEMA CATEGORIAL**
✓ Aplicar claves privadas al documento original para obtener la firma digital que se enviará	• La aplicación de claves privadas únicas emitidas por entidades certificadoras, asegurarán que la información enviada pueda ser leída únicamente por personas que tengan la clave pública correspondiente al documento original.	• Firma digital.	• Claves privadas y públicas. • Autoridades de certificación.

MATRIZ DE CONSISTENCIA ESPECÍFICA→ 5

PROBLEMA ESPECÍFICO.- Falta de control y seguridad en el acceso y utilización de los módulos del sistema.

OBJETIVO ESPECIFICO	HIPÓTESIS ESPECÍFICA	UNIDAD DE OBSERVACIÓN	SISTEMA CATEGORIAL
✓ Auditar cada una de las acciones realizadas en los módulos que conforman el sistema.	• Mediante la Auditoria que se realizara al sistema en funcionamiento se podrá tener un control permanente y más exhaustivo de las acciones que se realizan en cada uno de los módulos pertenecientes al mismo.	• Seguridad del software. • Auditoria informática.	• Análisis de riesgos y amenazas. • Técnicas de aseguramiento del sistema. • Auditoria de sistemas. • Objetivos y fines de la auditoria de sistemas. • Herramientas y técnicas para la auditoria de sistemas.

MATRIZ DE CONSISTENCIA ESPECÍFICA→ 6

PROBLEMA ESPECÍFICO.- Falta de control y seguridad en el acceso a personal no autorizado durante la utilización del sistema de gestión de documentos.			
OBJETIVO ESPECIFICO	**HIPÓTESIS ESPECÍFICA**	**UNIDAD DE OBSERVACIÓN**	**SISTEMA CATEGORIAL**
✓ Establecer e implantar niveles de seguridad y acceso en la aplicación que permitan el acceso únicamente a personal autorizado.	• El implantar niveles de seguridad al sistema, nos permitirá controlar el acceso de personas ajenas al mismo, evitando con ello que se realicen acciones inadecuadas tales como la manipulación de la información y alteración de la documentación existente en el Municipio de Calvas.	• Seguridad del software.	• Análisis de riesgos. • Amenazas. • Técnicas de aseguramiento del sistema. • Consideraciones de software.

MATRIZ DE OPERATIVIDAD DE OBJETIVOS ESPECÍFICOS→ 1

OBJETIVO ESPECIFÍCO.- Organizar los documentos de acuerdo a su índole de manera que se garantice eficiencia y eficacia durante su acceso.

ACTIVIDAD O TAREA	METODOLOGÍA	FECHA		RESPONSABLE	PRESUPUESTO	RESULTADOS ESPERADOS
		Inicio	Final			
✓ Realizar visitas para verificar la situación actual de los departamentos municipales. ✓ Centralizar los documentos de los diferentes departamentos municipales.	• Recolección de Datos utilizando una ficha ya establecida. • Observación directa de los procesos al tramitar un documento.	13/04/09	14/04/09	• Patricia Chamba • Franklin Andrade.	$ 30.00	• Documento que verifique los procesos de tramitación de documentos.
		15/04/09	16/04/09	• Patricia Chamba • Franklin Andrade.	$ 40.00	• Informe sobre como se realizará la centralización de la documentación existente en los diferentes departamentos.

✓ Clasificar los documentos de acuerdo a su índole.	• Entrevistas al personal. • Análisis cualitativo de la información. • Análisis y definición del proceso de etiquetación de los documentos ya clasificados	22/04/09	27/04/09	• Patricia Chamba • Franklin Andrade.	$ 40.00	• Documento que muestre como se realizó la organización y clasificación de los documentos de acuerdo a su tipo.
✓ Asignar un identificativo a los documentos de acuerdo a su tipo.		28/05/09	30/05/09	• Patricia Chamba • Franklin Andrade.	$ 30.00	• Informe que muestre las referencias establecidas para cada documento de acuerdo a su clasificación.

MATRIZ DE OPERATIVIDAD DE OBJETIVOS ESPECÍFICOS→ 2

OBJETIVO ESPECIFÍCO.- Generar certificados de autenticación que permitan firmar digitalmente la información que se enviará y recibirá entre los diferentes departamentos que conforman la institución

ACTIVIDAD O TAREA	METODOLOGÍA	FECHA		RESPONSABLE	PRESUPUESTO	RESULTADOS ESPERADOS
		Inicio	Final			
✓ Generar certificados de autenticación ✓ Usar las claves públicas y privadas asignadas por las entidades de certificación.	• Consultas bibliográficas al internet sobre certificados digitales • Definición de la entidad certificadora. • Tramitar el certificado digital con la entidad definida. • Seguir el proceso de autenticación definido por la entidad certificadora.	08/05/09	15/05/0	• Patricia Chamba • Franklin Andrade	$ 100.00	• Documento que indique cual es el formato utilizado para la obtención del o los certificados necesarios
		01/06/09	13/08/09	• Patricia Chamba • Franklin Andrade	$ 50.00	• Demostrar en el sistema como se utilizaran las claves asignadas, mediante un prototipo del producto final.

MATRIZ DE OPERATIVIDAD DE OBJETIVOS ESPECÍFICOS→ 3

OBJETIVO ESPECIFÍCO.- Usar funciones hash para generar datos asociados (huella digital) basados en la encriptación asimétrica o codificación de los documentos digitales.

ACTIVIDAD O TAREA	METODOLOGÍA	FECHA		RESPONSABLE	PRESUPUESTO	RESULTADOS ESPERADOS
		Inicio	Final			
✓ Utilizar funciones hash para obtener la huella digital. ✓ Encriptar el contenido del documento siguiendo el proceso definido en una encriptación asimétrica. ✓ Verificar si el contenido del documento ha sido encriptado correctamente	• Consultas bibliográficas al internet referidas a funciones hash y encriptación. • Definición del tipo de función hash que se utilizará. • Constatar los tipos de encriptación existentes. • Seguir el proceso establecido al utilizar algoritmos de encriptación asimétrica.	14/08/09	26/11/09	• Patricia Chamba • Franklin Andrade	$ 20.00	• Demostrar mediante un prototipo del sistema la generación de una huella digital al aplicar la función hash establecida.
		14/08/09	26/11/09	• Patricia Chamba • Franklin Andrade	$ 30.00	• Demostrar en el modulo del sistema correspondiente la encriptación correcta de los documentos digitales mediante el uso de algoritmos de encriptación asimétrica.
		14/08/09	26/11/09		$ 10.00	

MATRIZ DE OPERATIVIDAD DE OBJETIVOS ESPECÍFICOS→ 4

OBJETIVO ESPECIFÍCO.- Aplicar claves privadas al documento original para obtener la firma digital que se enviará

ACTIVIDAD O TAREA	METODOLOGÍA	FECHA		RESPONSABLE	PRESUPUESTO	RESULTADOS ESPERADOS
		Inicio	Final			
✓ Utilizar las claves públicas y privadas que se hayan generado	• Seguir el proceso de envío y recepción de información mediante claves públicas y privadas.	14/08/09	26/11/09	• Patricia Chamba • Franklin Andrade	$ 10.00	• Simulación del envío y recepción de información encriptada utilizando claves públicas y privadas.

MATRIZ DE OPERATIVIDAD DE OBJETIVOS ESPECÍFICOS→ 5

OBJETIVO ESPECIFÍCO.- Auditar cada una de las acciones realizadas en los módulos que conforman el sistema.

ACTIVIDAD O TAREA	METODOLOGÍA	FECHA		RESPONSABLE	PRESUPUESTO	RESULTADOS ESPERADOS
		Inicio	Final			
✓ Controlar el acceso a los módulos del sistema. ✓ Auditar cada una de las acciones realizadas. ✓ Obtener informes diarios de las actividades realizadas.	• Monitoreo de la utilización del sistema. • Seguir el proceso metodológico establecido en la auditoría de software que se realizará.	27/11/09	04/12/09	• Patricia Chamba • Franklin Andrade	$ 30.00	• Verificación en el sistema de los niveles de acceso previamente asignados.
		27/11/09	04/12/09	• Patricia Chamba • Franklin Andrade	$ 40.00	• Informe a través del sistema de cada una de las acciones que se realizan en la aplicación.
		27/11/09	04/12/09	• Patricia Chamba • Franklin Andrade	$ 20.00	• Informe detallado generado por el sistema concerniente a las acciones realizadas en cada módulo

MATRIZ DE OPERATIVIDAD DE OBJETIVOS ESPECÍFICOS→ 6

OBJETIVO ESPECIFÍCO.- Establecer e implantar niveles de seguridad y acceso en la aplicación que permitan el acceso únicamente a personal autorizado.

ACTIVIDAD O TAREA	METODOLOGÍA	FECHA		RESPONSABLE	PRESUPUESTO	RESULTADOS ESPERADOS
		Inicio	Final			
✓ Definir e implantar niveles de seguridad y acceso en la aplicación a desarrollarse. ✓ Verificar que la seguridad del sistema no haya sido vulnerada.	• Consultas bibliográficas al Internet referentes a la seguridad del software. • Seguimiento de normas para asegurar seguridad en los sistemas.	14/08/09	04/12/09	• Patricia Chamba • Franklin Andrade	$ 30.00	• Verificación de las condiciones de seguridad definidas en el sistema de manera tal que funcionen correctamente
		27/11/09	04/12/09	• Patricia Chamba • Franklin Andrade	$ 10.00	• Comprobación de accesos autorizados y no autorizados que se encuentren establecidos en la aplicación que se está desarrollando.

MATRIZ DE CONTROL DE RESULTADOS

NÚMERO	RESULTADOS	FECHA	FIRMA DIRECTOR DE TESIS
1	• Documento que verifique los procesos de tramitación de documentos.	14/04/09	
2	• Informe que contenga la forma en que se realizará la centralización documentos	16/04/09	
3	• Documento que muestre la organización de documentos de acuerdo a su tipo.	27/04/09	
4	• Informe que muestre las referencias establecidas para cada documento	30/05/09	
5	• Documento que indique el formato utilizado para la obtención de certificados digitales	15/05/09	
6	• Demostrar en el sistema como se utilizaran las claves asignadas, mediante un prototipo del producto final	13/08/09	
7	• Demostrar mediante un prototipo del sistema la generación de una huella digital al aplicar la función hash establecida.	26/11/09	

8	• Demostrar en el modulo del correspondiente la encriptación de documentos mediante el uso de algoritmos de encriptación asimétrica.	26/11/09	
9	• Simulación del envío y recepción de información encriptada utilizando claves públicas y privadas.	26/11/09	
10	• Verificación en el sistema de los niveles de acceso previamente asignados.	04/12/09	
11	• Informe a través del sistema de cada una de las acciones que se realizan en la aplicación.	04/12/09	
12	• Informe detallado generado por el sistema concerniente a las actividades realizadas en cada módulo del mismo.	04/12/09	
13	• Verificación de las condiciones de seguridad definidas en el sistema.	04/12/09	
14	• Comprobación de accesos autorizados y no autorizados que se encuentren establecidos en la aplicación que se está desarrollando.	04/12/09	

ANEXO 8:

CONFIGURACIONES PARA FUNCIONAMIENTO DE LA APLICACIÓN EN EL SERVIDOR

La configuración que a continuación detallamos está definida para un Servidor con Sistema Operativo Windows Server 2003/2008; esto debido a que el Municipio de Calvas actualmente dispone del Sistema Operativo Windows Server 2003 con licencia, manifestando en lo posterior que piensan migrar al 2008.

Nuestra aplicación cuenta con un módulo de Respaldos, el cual se encarga de generar respaldos de la base de datos, archivos de imagen y archivos subidos al servidor, además de permitir restaurar o eliminar dichos respaldos que son almacenados en una carpeta destino cuya ruta se haya establecido previamente a través del módulo Parámetro.

El proceso de respaldo de la información lo hemos logrado gracias a la utilización del siguiente comando:

```
String comnado = "cmd /c mysqldump --opt --user="+ ServicioApplication.usuarioBasedatos+" --password=" + ServicioApplication.claveBasedatos+ " " + ServicioApplication.nombreBasedatos;
```

Estas líneas de código nos permiten obtener los respaldos directamente pero utilizando comandos propios de windows, lo cual influye considerablemente para que la aplicación no pueda ser ejecutada bajo la plataforma Linux.

En lo que se refiere al equipo cliente el Sistema Operativo que se utilice será independiente, ya que su objetivo es de enviar peticiones que serán receptadas por el servidor.

Para que la aplicación sea ejecutada requiere de ciertos recursos hardware y software. En lo que a software se requiere es necesario una vez instalado el Sistema Operativo y el jdk 1.5.0; configurar la variable de entorno, esto con la finalidad de evitar mensajes de error en donde se indica que no se reconoce como comando externo; el servidor Apache Tomcat 6.014, Mysql 5.0 y finalmente configuración del puerto https.

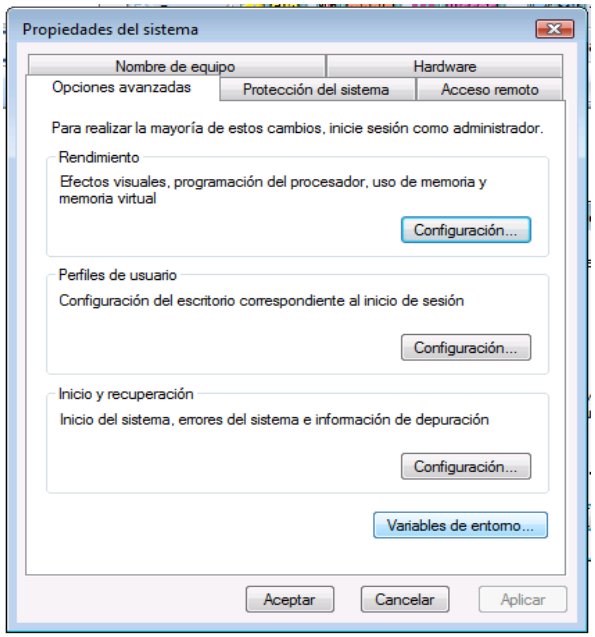
1. CONFIGURACIÓN DE LA VARIABLE DE ENTORNO

Software Requerido: jdk-1. 5. 0 previamente instalado.

Para que Windows reconozca la carpeta de nuestro jdk debemos notificarle a través de lo que se conoce como variables de entorno, que no son más que variables que almacenan configuraciones y direcciones de nuestro sistema como carpeta de usuarios, direcciones de librerías o recursos del sistema, etc. Las librearías y aplicaciones de Java serán reconocidas por Windows para que se puedan ejecutar en cualquier parte de nuestros directorios, para esto vamos a darle valor a las variables de entorno, Path y Classpath.

Configuración de la variable de Entorno Path

Le damos click derecho a Mi PC y en el menú emergente seleccionamos propiedades



Luego seleccionamos la pestaña que dice Opciones Avanzadas, dentro de opciones avanzadas hay un botón Variables de Entorno y le damos click. Buscamos la sección que dice Variables de Usuario (en la parte superior de la ventana) y le damos click a Nueva y asignamos lo siguiente:

Nombre: **JAVA - HOME**

Valor: **C:\Archivos de Programa\Java\jdk-1_5_0_12\bin**

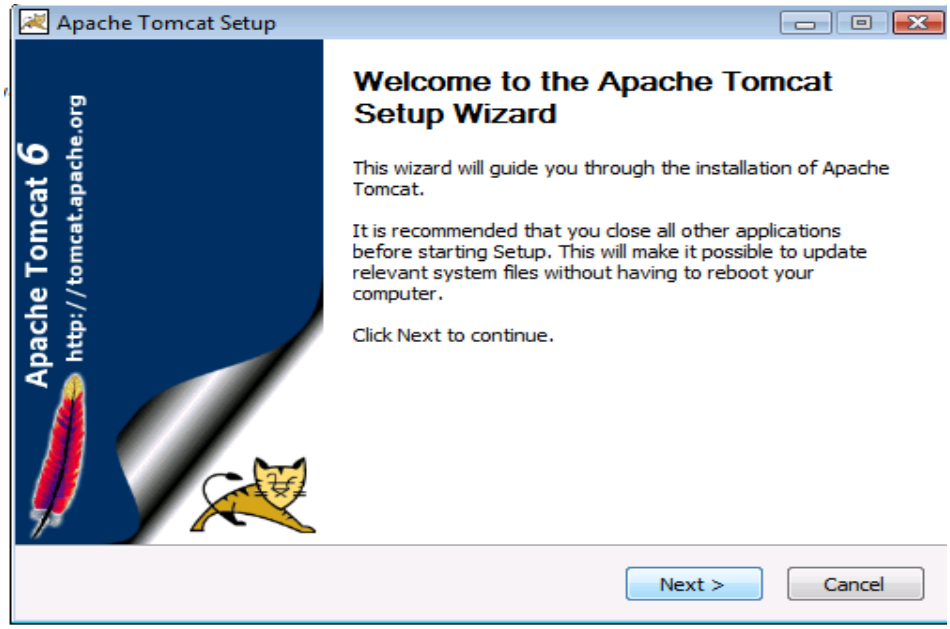
Luego buscamos la variable Path, y elegimos Editar; y al final del valor de esta variable asignamos:

; %JAVA – HOME% \bin

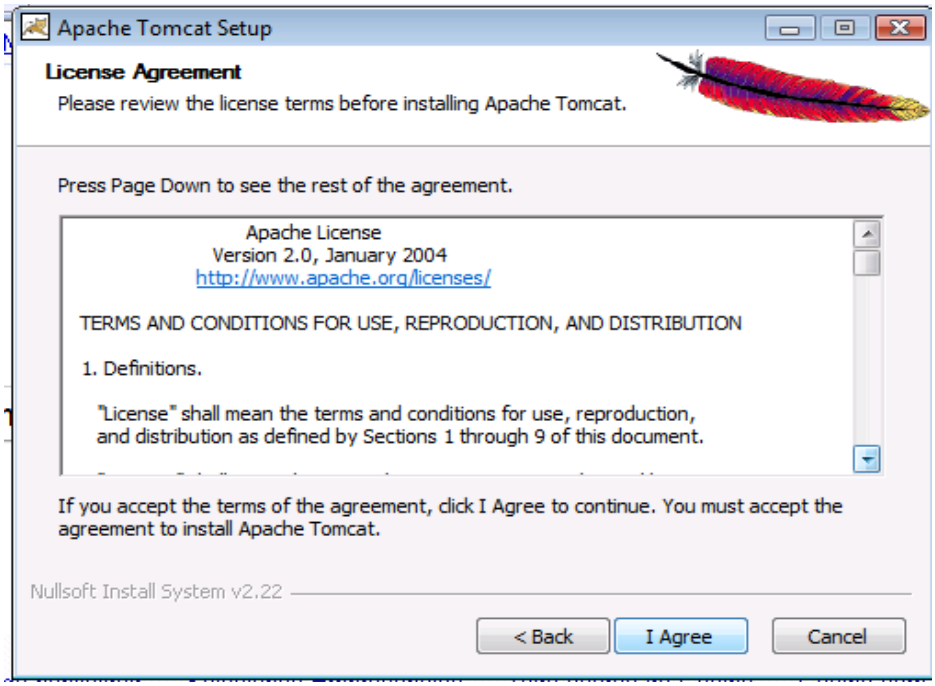
Y finalmente luego de ello click en Aceptar

2. INSTALACIÓN DE APACHE TOMCAT 6.0.14

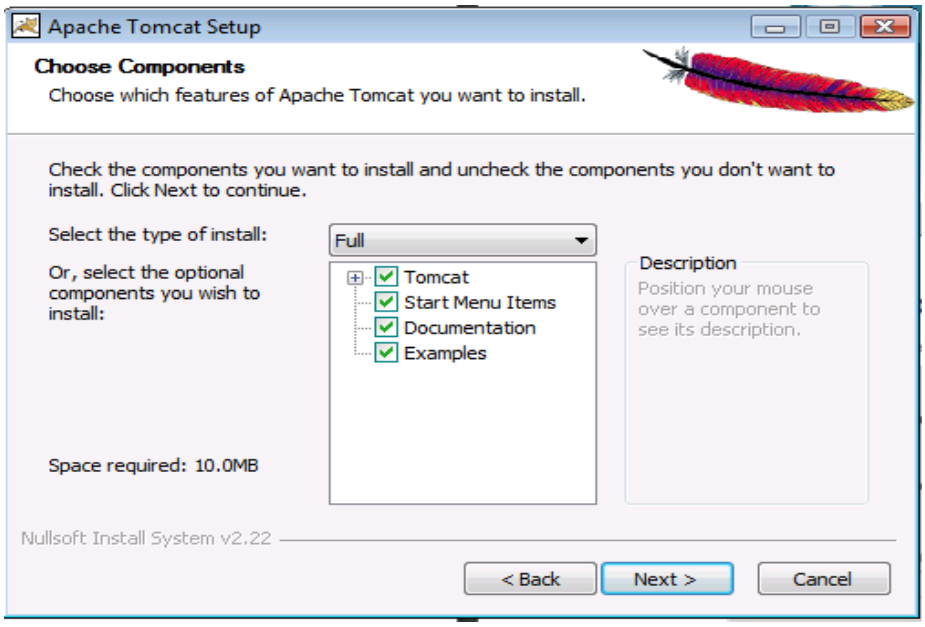
Para instalar Apache Tomcat, en primer lugar ejecutamos el archivo apache-tomcat-6.014.exe. En la ventana que aparecerá click en Next



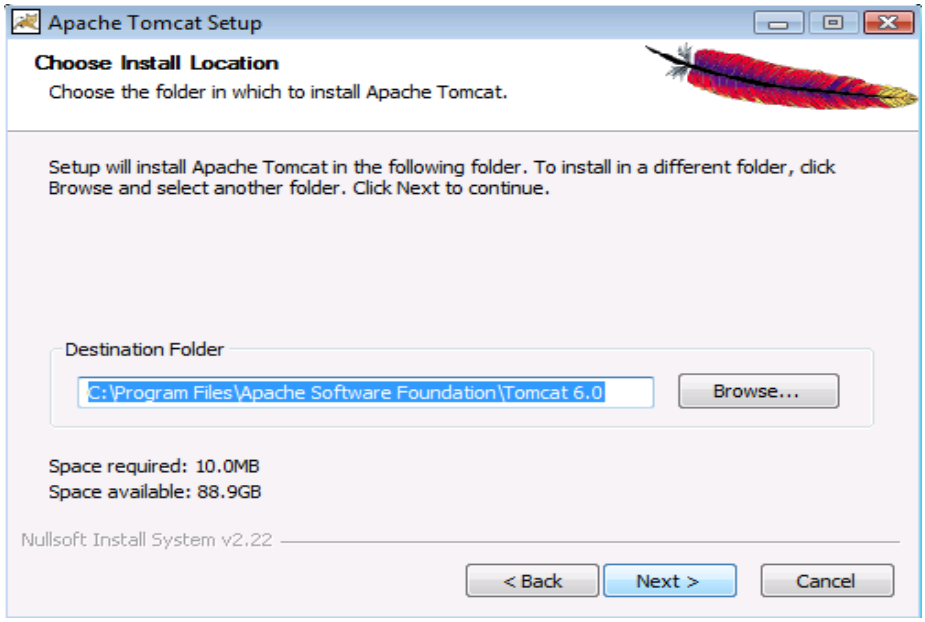
Luego click en I Agree



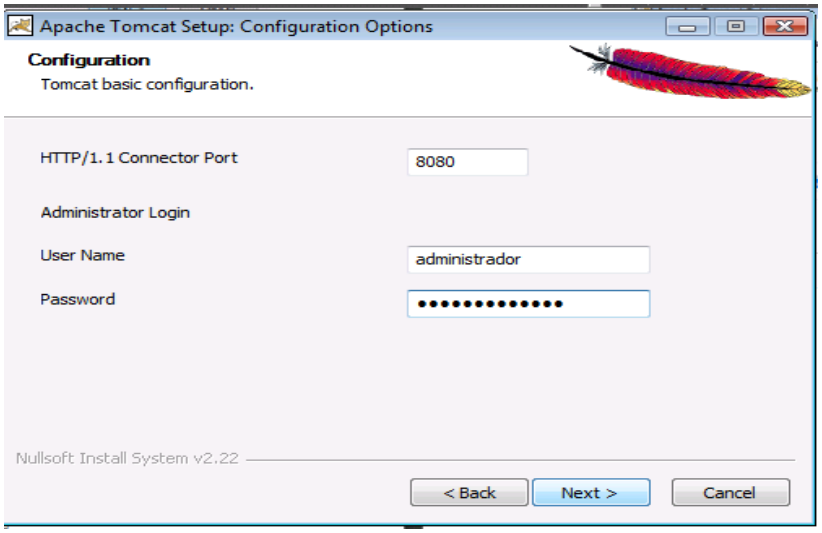
En el tipo de instalación elegimos la opción Full y click en Next



En la siguiente ventana nos mostrará la ruta en donde se instalará Apache Tomcat, dejamos la instancia por defecto y click en Next

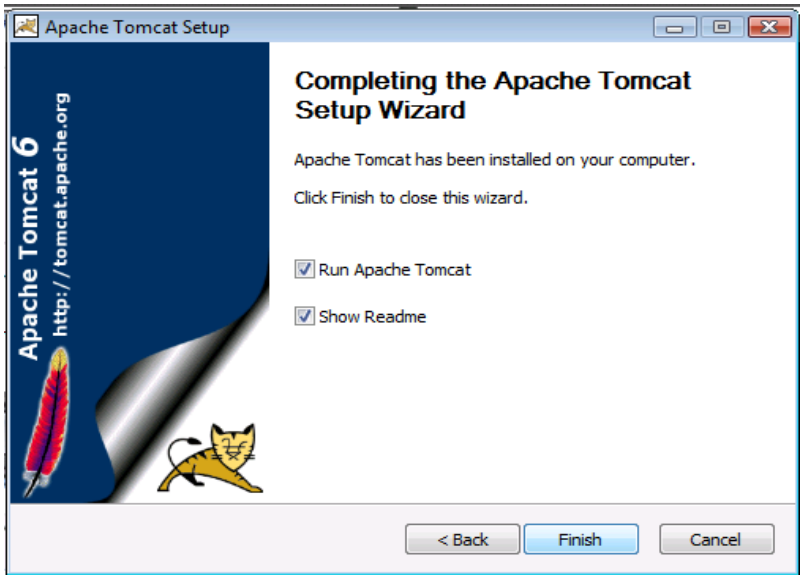


A continuación digitamos en nombre de usuario <administrador> y contraseña <administrador>, el puerto seguirá siendo el 8080, click en Next



En la siguiente ventana nos mostrará simplemente la ruta del jdk que previamente habíamos instalado y configurado, click en Install.

Luego de ello la instalación iniciará y concluirá en unos minutos, para finalmente presentar la ventana en la que damos click en Finish



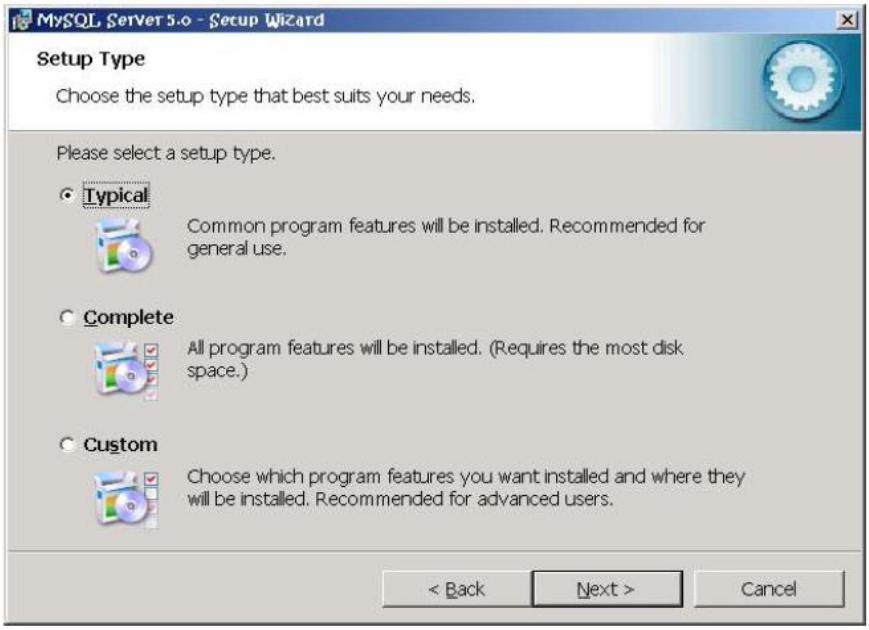
En la barra de herramientas del escritorio, se añadirá un icono en el cual se indica que el servicio de Apache Tomcat ha iniciado o se está ejecutando.

3. INSTALACIÓN DE MYSQL 5.0

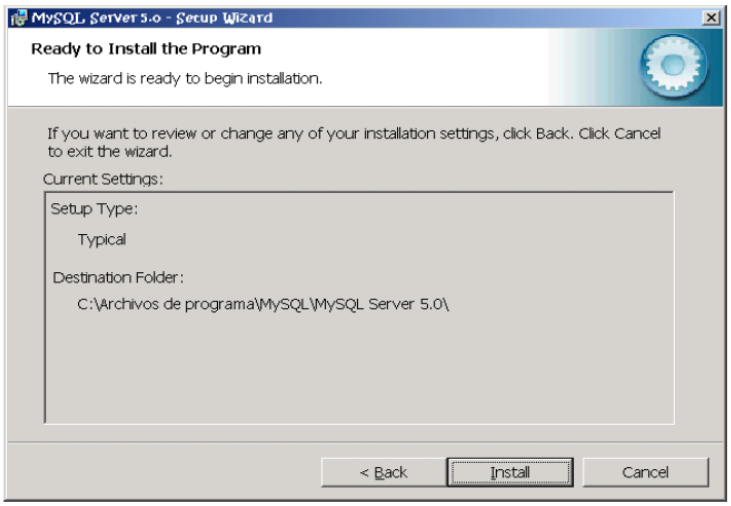
El primer paso es ejecutar el archivo Setup.exe

Aquí se espera unos minutos mientras se cargan los archivos necesarios para la instalación hasta que aparece la siguiente pantalla:

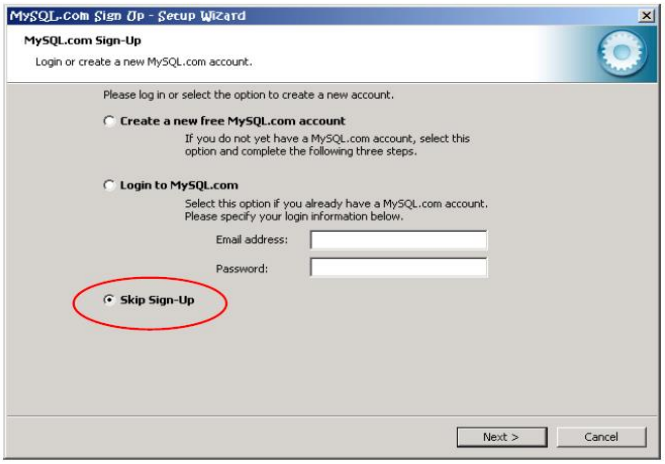
Se presiona Next y aparece la pantalla



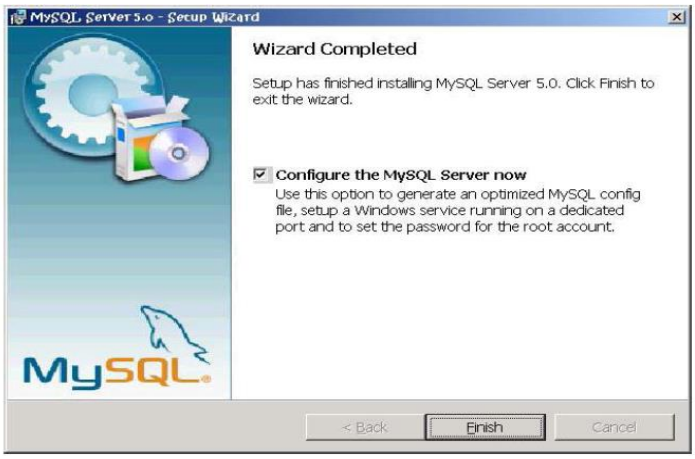
Se selecciona el tipo de instalación Typical y se presiona Next aparecerá la siguiente pantalla: (si se quiere instalar algunos componentes o realizar la instalación en otra ubicación que no sea por defecto seleccione Custom y siga las instrucciones).



Se presiona Install. Luego de esto aparece la siguiente pantalla, se selecciona la opción Skip Sign-Up y se presiona Next.

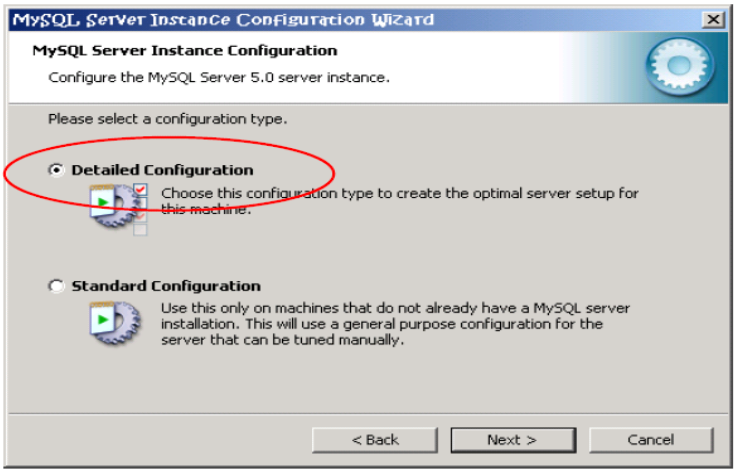


Y finaliza la primera parte de instalación

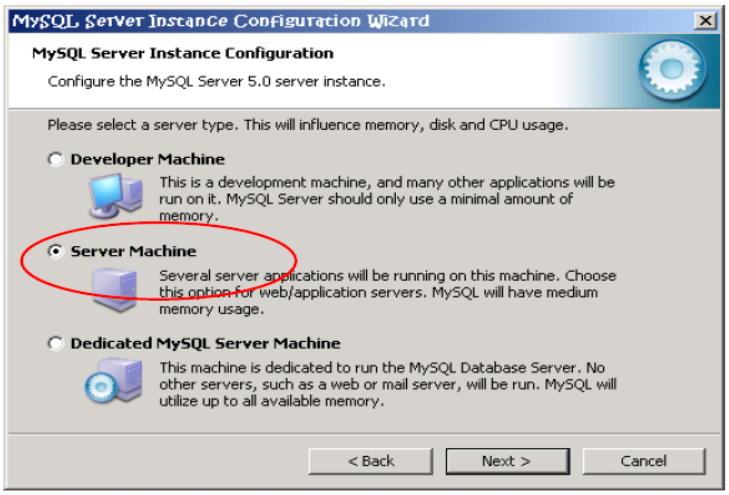


Se presiona Finish y se continua con la configuración del servidor MySQL

Se selecciona el tipo de configuración detallada para la nueva instancia

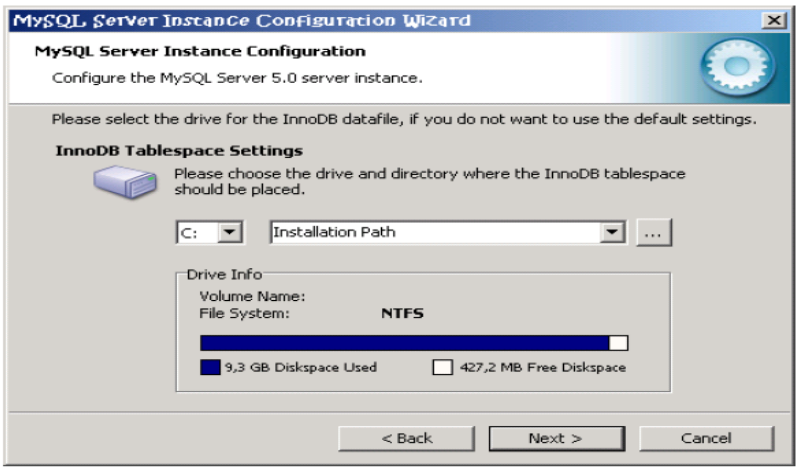


Se presiona Next, como se va a crear como servidor se selecciona la opción Server Machine y se presiona Next

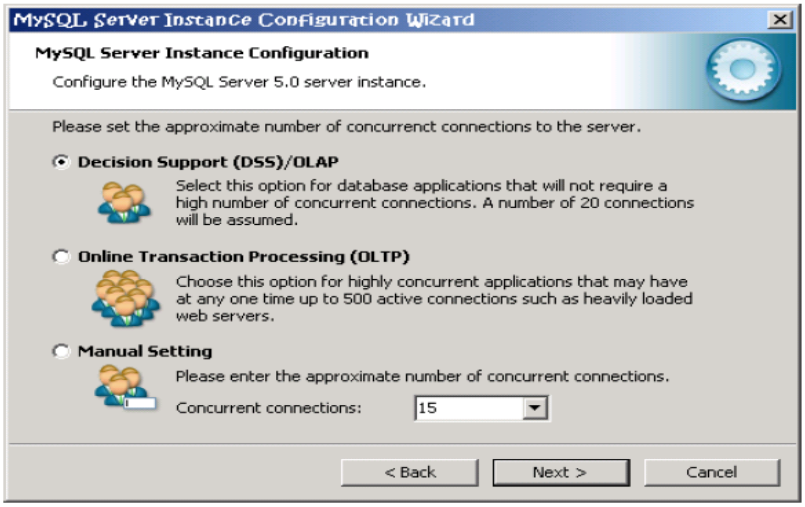


Se selecciona la base de datos Multifuncional o base de datos de propósito general

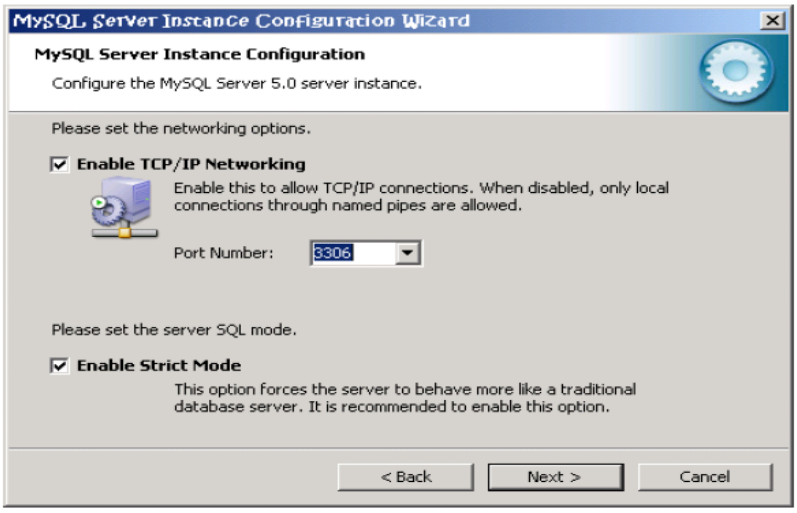
Por defecto el tablespace es ubicado en la ruta C:, presionar Next



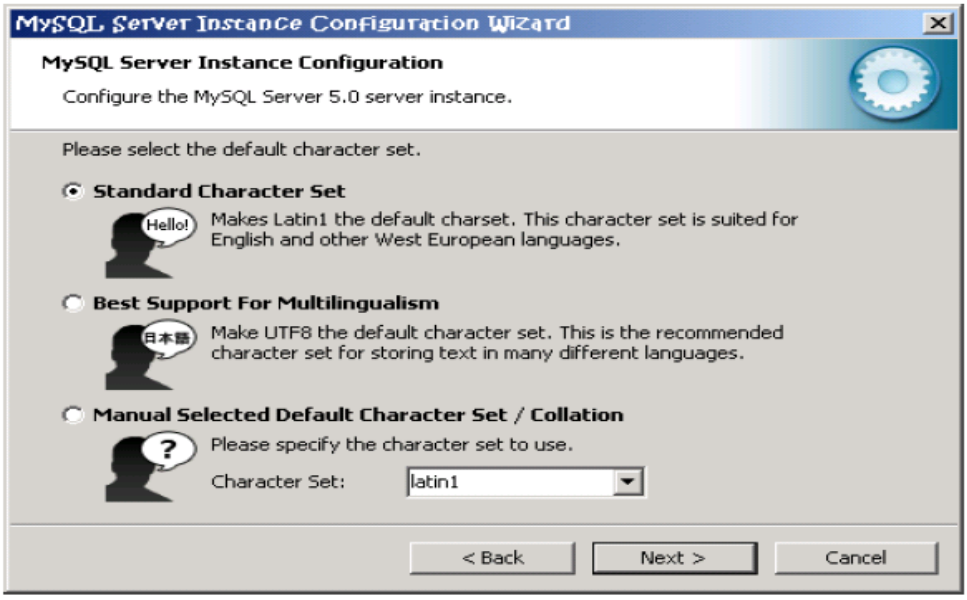
Seleccionar el número de conexiones concurrentes al servidor, por defecto OLAP (On Line Análisis Process), presionar Next:



Ahora se selecciona el protocolo de comunicación de red y su numero de puerto, por defecto es TCP/IP y el numero de puerto 3306, además se habilita modo estricto, presionar Next:



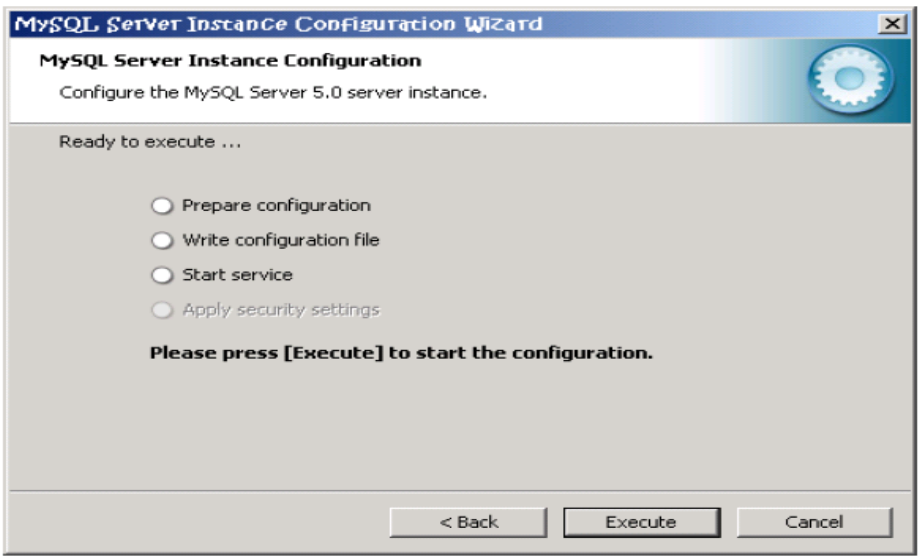
Seleccionar juego de caracteres, se deja por defecto la opción de caracteres estándar, presionar Next:



Se instala el nuevo servicio y su respectivo nombre, este servicio será iniciado automáticamente, presionar Next:

Luego de, ello establecimos una contraseña para el “super usuario” root, se chequea la caja y se escribe la contraseña y su confirmación, presionar Next

Se termina la configuración del servidor MySQL5, para ello presionar Execute y se inicia el servicio.



Presionar Finish y se termina el asistente de configuración del servidor MySQL 5.

4. CONFIGURACIÓN DEL PUERTO HTTPS

Una vez instalado el servidor Apache Tomcat, vamos a redireccionar el puerto 8080 al 8443 conocido como puerto de seguridad a través de la generación de un archivo .keystore, el cual nos permitirá llevar a cabo este proceso. Para ello en primer lugar debemos ingresar el cmd y digitar la ruta en donde se encuentra instalado el jdk 1.5.0, y escribir la siguiente sentencia:

C:\Archivos de programa\Java\jdk1.5.0\bin\keytool.exe -genkey -alias tomcat -keyalg RSA

Con este comando y sus argumentos, estamos ordenando que generaremos un nuevo certificado o una nueva key, con el alias tomcat. Luego nos pedirá una serie de datos que son los que conformarán el almacén de claves. La clave que viene por defecto con el alias de tomcat es:

changeit

En nuestro caso cuando nos solicite la clave digitaremos administrador. Cuando se termine de ingresar toda la información se debe digitar OK para que se valide. Al finalizar este paso el KeyTool genera un archivo que almacena la llave, es decir un .keystore. En nuestro caso en Windows Server se alojó en:

C:\User\Administrador

Si estuviéramos utilizando Windows XP: C:\Documents and Settings\Usuario

Windows Vista: C:\User\Usuario

Ahora debemos configurar el servidor Tomcat para aceptar y habilitar el puerto SSL, que por defecto es el 8443. Dentro de la carpeta del apache-tomcat-6.0.14, nos dirigimos <conf> localizamos el archivo server.xml y descomentamos unas líneas que aparecen por defecto con carácter de comentarios o en su defecto las digitamos y le agregamos un atributo para indicar cuál será el keystore, de esta manera:

```
<Connector

        port="8443" minSpareThreads="5" maxSpareThreads="75"
        enableLookups="true" disableUploadTimeout="true"
        acceptCount="100"  maxThreads="200"
        scheme="https" secure="true" SSLEnabled="true"
```

keystoreFile= " *C:\User\Administrador*\.keystore, keypass administrador”
clientAuth="false" sslProtocol="TLS"
/>

En keystoreFile debemos digitar la ruta en donde se encuentra nuestro archivo generado, que anteriormente indicamos.

Luego de agregar estas líneas guardamos los cambiamos y hemos finalizado la configuración del puerto https.

Es importante recordar que la primera vez que tratemos de ejecutar la aplicación una vez habilitado el puerto 8443, debemos añadir la excepción que nos aparecerá en el navegador, y generar el certificado que nos indique, luego de ello la aplicación se desplegará sin ningún problema.

OTRAS CONSIDERACIONES

Crear la base de datos: <firmas>

Archivo war o aplicación: SGD –GADCC (Ver Ejecución Manual de Usuario Programador)