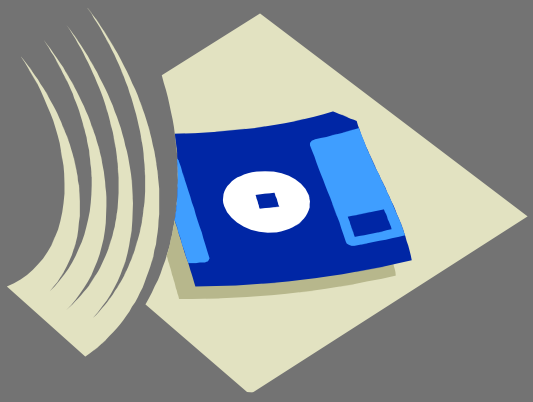
Registro de incidencias

Seguridad en ficheros automatizados. Protección de datos de carácter personal (DD.CC.PP.)

Tal y como establece el artículo 90 del Real Decreto 1720/2007, todo fichero automatizado deberá contar con un registro de incidencias en el que se hará constar cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos de carácter personal.



Autora: Mayte Medina Gutiérrez
Consultor: Juan José Cuadrado Gallego
TFC Ingeniería del Software 2º Sem. 2012

03/10/2012

Contenido

DEDICATORIA.

A mi madre y a mi hija, por ellas emprendí este camino, y siempre me han acompañando.

A todas la personas que me han animado a seguir hasta llegar al final.

GRACIAS.

1. Introducción

Las medidas de seguridad aplicables en los ficheros automatizados se encuentran reguladas en los artículos 89 a 104 del reglamento que desarrolla la Ley Orgánica de Protección de Datos (Real Decreto 1720/2007)- LOPD.

La protección de datos

El derecho a la protección de datos personales es un derecho fundamental de todas las personas, que se traduce en la potestad de control sobre el uso de sus datos personales. Este control permite evitar que, a través del tratamiento de nuestros datos, se pueda disponer de información sobre nosotros que afecte a nuestra intimidad y demás derechos fundamentales y libertades públicas.

Articulo 18 de la Constitución Española:

"La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Obligatoriedad de la Ley

Esta ley obliga a todas las personas, empresas y organismos -tanto privados como públicos que dispongan de datos de carácter personal- a cumplir una serie de requisitos y aplicar determinadas medidas de seguridad en función del tipo de datos que posean.

Agencia Española de protección de datos

Entidad encargada de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

1.1. Identificación del proyecto

Modelo de documento de seguridad

La Agencia Española de Protección de Datos, ha publicado una guía de protección de datos en la que se desarrolla el modelo del documento de seguridad, con objeto de recopilar las exigencias mínimas que establece el Reglamento de la LOPD, estructurado como sigue:

1. Ambito de aplicación
2. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento
3. Información y obligaciones del personal
4. Procedimientos de notificación, gestión y respuesta ante las incidencias
5. Procedimientos de revisión

El estudio de este proyecto se centra en el punto 4 , para lo cual se pretende desarrolla el registro de incidencias.

Articulo 90 de RD 1720/2007 de LODP

Tal y como estable el artículo 90 del Real Decreto 1720/2007, todo fichero automatizado deberá contar con un registro de incidencias en el que se hará constar cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos de carácter personal en los siguientes términos:

"Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas."

Descripción del proyecto: Registro Automatizado del Incidencias.

El proyecto de Registro Automatizado de Incidencias tiene como objeto el desarrollo de un software que permita realizar el procedimiento de notificación, gestión y respuesta ante las incidencias.

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en el Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal.

El procedimiento a seguir para la notificación de incidencias será el siguiente:

El proceso se inicia cuando un usuario detecta que se ha producido una incidencia de seguridad. El usuario se deberá identificar para acceder al sistema y realizar la comunicación de la incidencia. El sistema proporcionará una lista de incidencias tipo más comunes de entre las cuales seleccionará, en caso de que la incidencia fuera de otra índole se procederá a su descripción.

Posteriormente se introducirá todos aquellos datos referentes a la incidencia que son requeridos y establecidos en el modelo el documento de seguridad editado por la Agencia de Protección de datos.

En el caso de que la incidencia conlleve para su resolución la recuperación de datos el proceso deberá contemplar dicha actuación.

Por último el procedimiento deberá indicar el estado en que han que dado los archivos y soporte afectado por la incidencia producida.

El responsable de seguridad del fichero afectado se encargará de solucionar la incidencia con toda la urgencia que le sea posible. No se especifica la forma de gestionar las incidencias debido a la propia naturaleza de estas, por lo que el responsable del fichero deberá tomar la decisión que considere más oportuna dependiendo de la naturaleza de la incidencia, y actuar en base a la decisión tomada de inmediato.

1.2. Objetivos del proyecto

El Reglamento de la LODP permite realizar el registro de incidencias mediante el rellenado de formularios en soporte papel si este no está informatizado.

El proyecto de informatización del registro de incidencias tiene como objeto :

. Contribuir a la implantación de la **Oficina sin papeles,** como metodología avanzada de reducción del consumo de materias primas – papel -, mediante la utilización de las tecnologías disponibles.

. Servir de canal de comunicación, en donde interactúen el responsable de seguridad y las personas que notifican las posibles incidencias, de forma rápida y eficaz.

. El proyecto en general persigue la eficiencia, en el procedimiento de gestión de incidencias, con la reducción de gastos y el incremento la capacidad de respuesta.

1.3 Entorno tecnológico

Se ha optado por el entorno tecnológico y operativo utilizado para la realización del proyecto la tecnología orientada a objetos, utilizando Java como lenguaje de programación, RMI (Java Remote Method Invocation) como mecanismo para acceder a las operaciones del sistema de forma remota, y proporcionando a los usuarios una interfaz muy clara y amigable.

1.4 Requerimientos técnicos

Se pretende desarrollar el proyecto utilizando un entorno distribuido cliente/servidor, por las ventajas que aporta en cuanto a que permite que la información se procese cerca de donde se genera, facilidad de uso de interfaces gráficas de usuario.
Para el desarrollo y documentación del proyecto, en el aspecto tecnológico se propone los siguientes software y herramientas de desarrollo y diseño:

1. RMI de Java que nos permite desarrollar aplicaciones distribuidas.

2. JDK 6, que proporciona un entorno de multiplataforma, y como único requisito el cliente debe disponer de una máquina virtual Java.

3. NetBeans IDE 7.0.1. IDE con Swing , herramienta necesaria para el diseño de la interfaz de usuario y la posterior implentación del código.

4. MagicDraw como editor UML., software herramienta de diseño que nos facilitará el modelado de los casos de uso , clases y secuencia…etc.

5. Gestor de base de datos: PostgreSQL v.9.0, gestor de base de datos relacional donde se definirán la base de datos y estructura de tablas necesaria para contener los datos.

1.5 Metodología

El proyecto se va a desarrollar siguiendo el método del ciclo de vida clásico o en cascada, al ser una metodología donde cada una de las etapas se desarrolla de manera lineal facilita la realización de este proyecto.

En este documento solamente se van llevar a cabo las dos primeras fases: análisis de requerimientos y diseño técnico y servirá como la base para las siguientes fases de desarrollo de software.

El inconveniente que presenta el ciclo de vida en cascada en la fase de análisis de requisitos, por el hecho de que fácilmente suelen ser incompletos, no afectaría inicialmente al proyecto que nos ocupa, ya que los requisitos están claramente definidos en el modelo de documento de seguridad para comunicación de incidencias en ficheros que afecten a datos de carácter personal.

1.6 Planificación

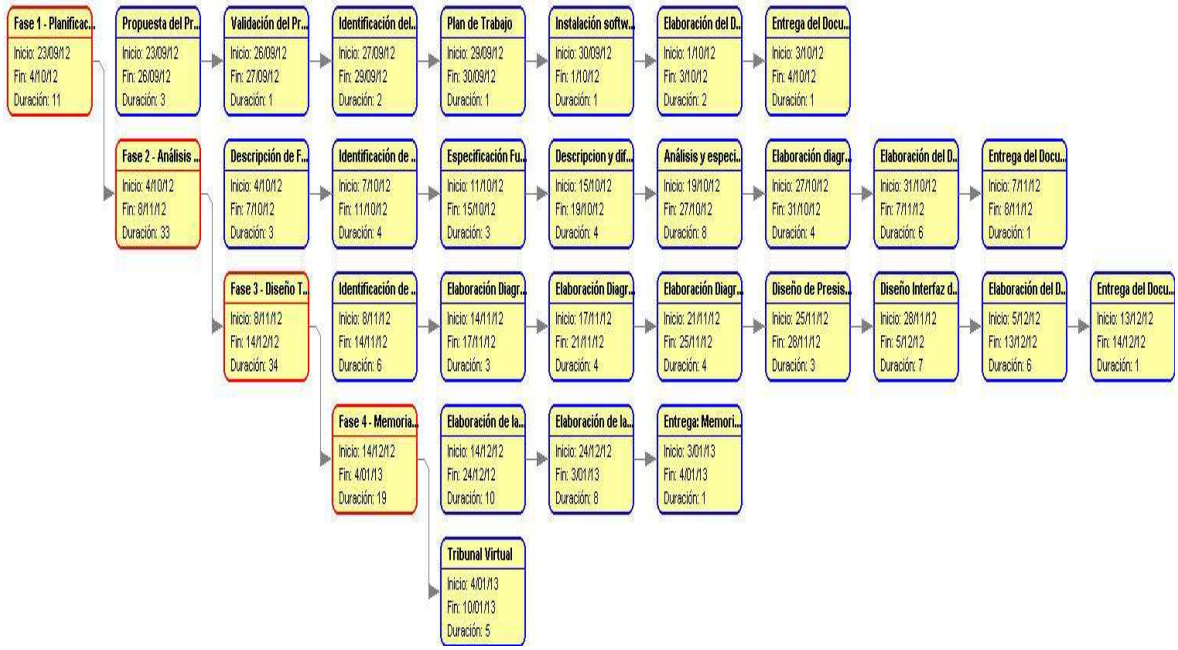
El proyecto ha sido organizado teniendo en cuenta las fechas de entrega de las PECs propuestas por el aula de TFC – Ingeniería del Software de la UOC. La planificación ha sido pensada en que habrá una dedicación constante, incluyendo los días del fin de semana. Este documento engloba las diferentes fases del proyecto con los siguientes hitos:

1. Inicio: 23 de septiembre de 2012. Hito 1
2. Documento PEC1 Planificación: 3 de octubre de 2012. Hito 2
3. Documento PEC2 Análisis de Requerimientos: 7 de noviembre de 2012. Hito 3
4. Documento PEC3 Diseño técnico: 12 de diciembre de 2012. Hito 4
5. Memoria y presentación del proyecto: 2 de enero de 2013. Hito 5
6. Tribunal virtual: 25 de enero de 2013. Hito 6

En la planificación y duración de este proyecto no se incluyen la fases de Implementación del sistema ni la fase de Testing y análisis de calidad.

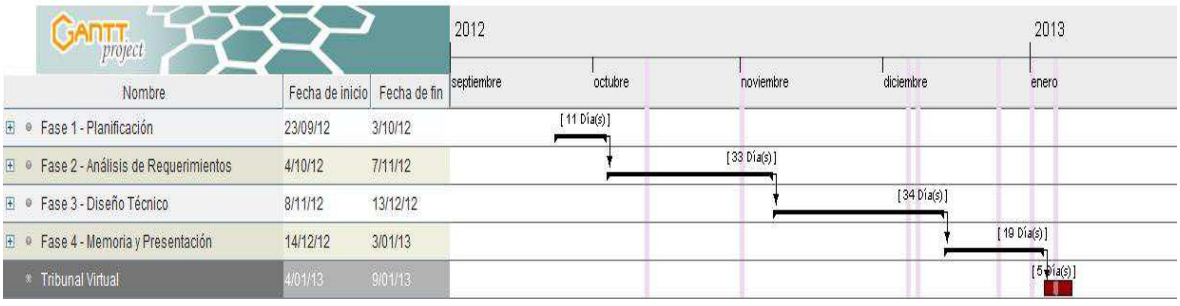
1.6.1. Descomposición y asignación de tareas

Diagrama de PERT: de forma grafica se puede observar las fases del proyecto y las distintas tareas a realizar en cada una de estas fases, así como el periodo entre fechas a realizar dichas tareas.



1.6.2. Diagramas de Gantt

General: fases y periodos.



Fase 1: Planificación.

Propuesta del proyecto

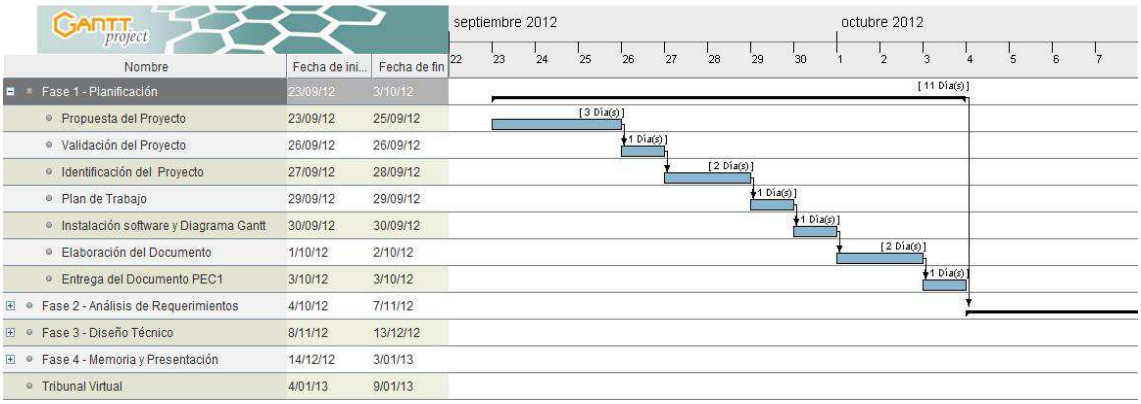
Aceptación del proyecto

Descripción general del proyecto y justificación

Base legal

Objetivos

Planificación de tareas



Fase 2: Análisis de Requerimientos

Descripción detallada de funcionalidades

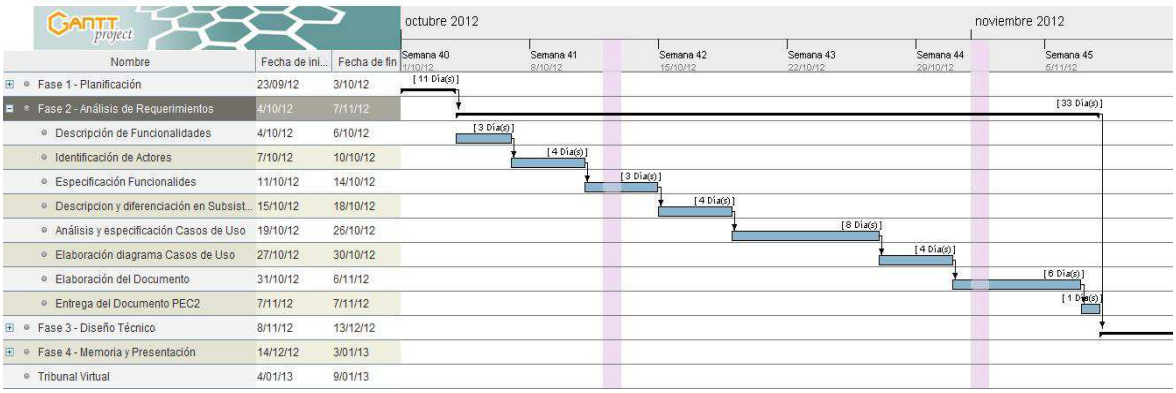
Identificación da Actores

Especificación de Funcionalidades

Descripción y diferenciación de subsistemas

Análisis y especificación de casos de uso

Elaboración diagrama casos de uso



Fase 3: Diseño Técnico

Identificación de Clases y Jerarquías

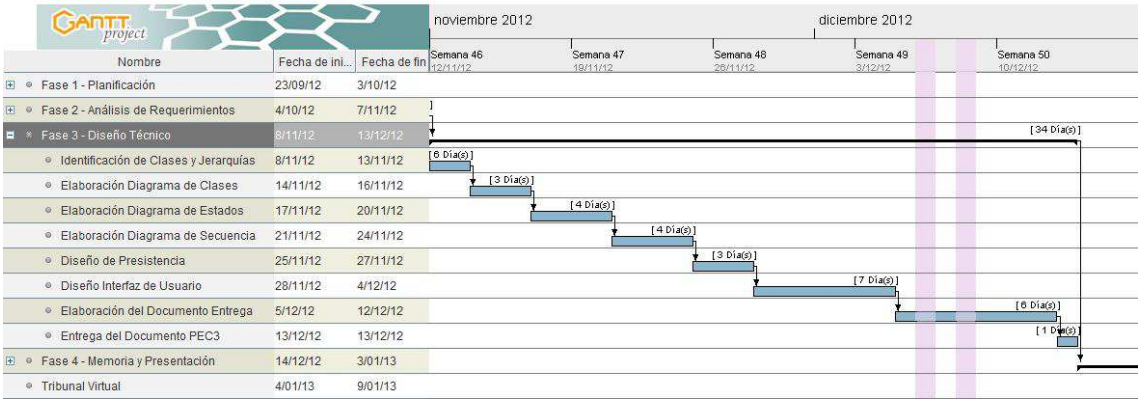
Elaboración de diagrama de Clases

Elaboración del diagrama de Estado

Elaboración del diagrama de Secuencia

Diseño de persistencia

Diseñar Interfaz de Usuario

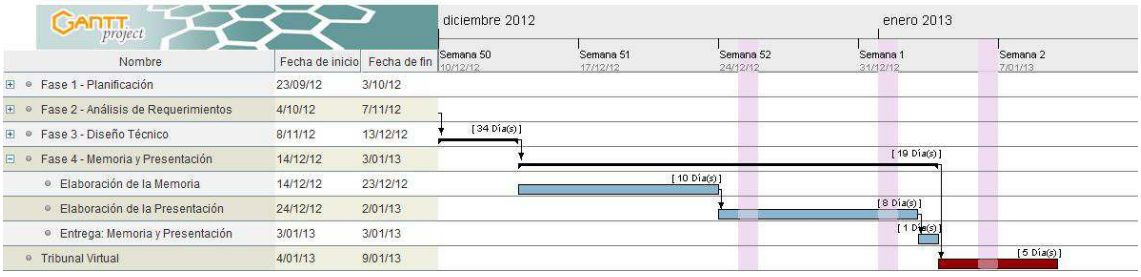


Fase 4 y Tribunal Virtual:

Elaborar la Memoria del proyecto

Elaborar una Presentación del proyecto

Exposición del proyecto: Tribunal Virtual



2. Análisis de Requerimientos. Introducción.

Esta fase de análisis de requerimientos o requisitos tiene como objetivo definir con detalle las necesidades de información para el desarrollo del software objeto del proyecto que nos ocupa.

El conocimiento necesario del dominio de la aplicación, que nos permita precisar las funciones y los requisitos en general del software, está basado en la recogida de información del las siguientes fuentes:

Medidas de seguridad en ficheros automatizados reguladas en los artículos 89 a 104 del reglamento que desarrolla la LOPD (Ley Orgánica de Protección de Datos 15/1999 - Real Decreto 1720/2007. Las medidas de seguridad aplicables a los ficheros están clasificadas en tres niveles:

- **Nivel básico:** Las medidas correspondientes al nivel básico se aplican a todos los ficheros
- **Nivel medio:** Las medidas del nivel básico más las de nivel medio se aplican a aquellos ficheros que requieren de un nivel medio de seguridad.
- **Nivel alto:** Todas las medidas de seguridad se aplican a aquellos ficheros que requieren de un nivel alto de seguridad.

Disponer de un registro de incidencias es de obligado cumplimiento para los niveles medio y alto.

Guía Modelo del Documento de Seguridad, publicada por la Agencia Española de Protección de Datos. En el apartado 4. se desarrolla los procedimientos de notificación, gestión y respuesta ante incidencias de seguridad en ficheros automatizados.

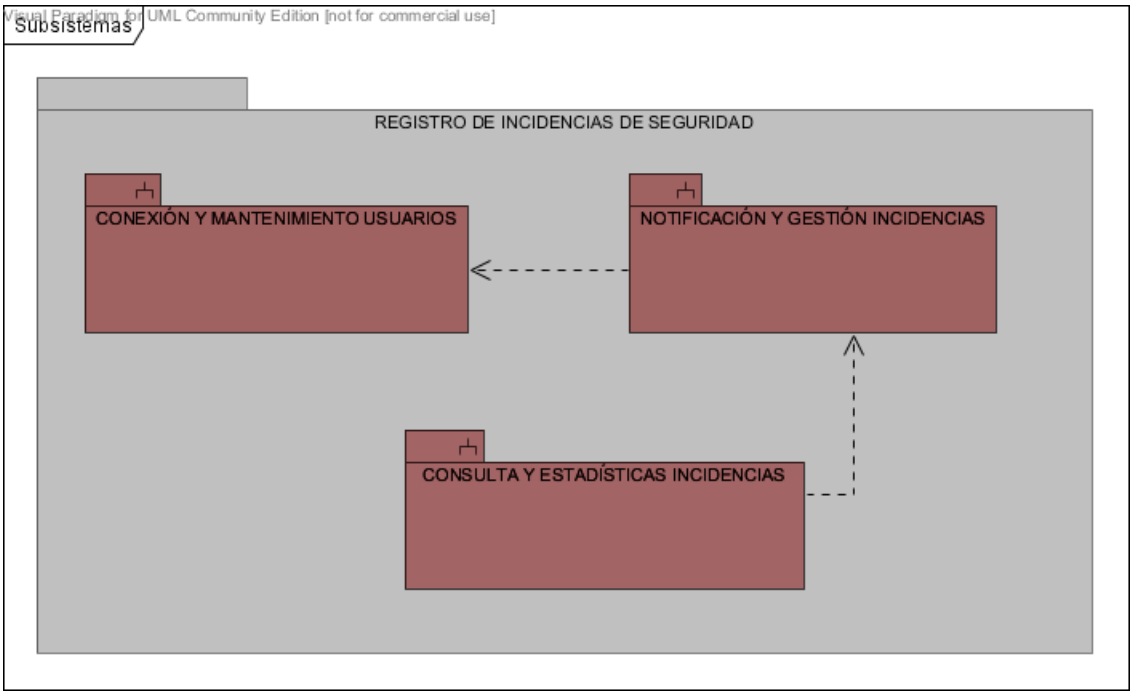
El registro de incidencias es una herramienta indispensable en todo sistema de información, este forma parte del documento de seguridad de cualquier empresa o administración donde se trata con ficheros que contienen datos de carácter personal, y por tanto deberá estar a disposición de los funcionarios de la AEPD (Agencia Española de Protección de Datos), en caso de inspección si estos lo requieren.

2.1. Descripción de funcionalidades.

El registro de incidencias tiene como objeto crear un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal, así como dejar constancia de la adopción de las medidas correctoras para que dicha incidencia sea controlada, por lo que debe mantenerse una acción permanente de control, revisión y actuación sobre las medidas implantadas e incidencias detectadas.

En el registro de incidencias deben quedar registrados todos aquellos problemas ocurridos en el sistema de información, de forma que nos permita por un lado evitar que se produzcan de nuevo y en caso de repetirse, poder disponer de un histórico de soluciones adecuadas para una mayor rapidez en la resolución de la incidencias que se detecten. El histórico deberá contener un conjunto de incidencias tipificadas así como la resolución asignada al tipo de incidencia.

El procedimiento de registro de incidencias lo podemos descomponer en tres subsistemas diferenciados, por una parte el subsistema de conexión, el subsistema de gestión de incidencias y el subsistema de consultas y estadísticas.



2.2.1. Subsistema de conexión y mantenimiento.

En este subsistema se desarrolla el mantenimiento de usuarios para acceder al sistema. Se tienen en cuenta las medidas y normas relativas a la autenticación de los actores intervinientes en el sistema.

La identificación de los usuarios se debe realizar de forma inequívoca y personalizada verificando su autorización, a cada usuario se le asigna un rol según las funciones asignadas dentro del sistema.

Las operaciones son las siguientes:

- Alta de usuario
- Baja de usuario
- Modificación de usuario
- Conexión al sistema

2.2.2. Subsistema de notificación y gestión de incidencias.

En este subsistema se desarrolla la comunicación de incidencias identificado el usuario que la registra, así como procedimientos de gestión necesarios para solventar la incidencia.

Las operaciones son las siguientes:

- Alta comunicación de incidencia.
- Modificación comunicación de incidencia
- Petición: resolver incidencia
- Resolver incidencia.
- Cerrar incidencia

2.2.4. Subsistema de consulta y estadísticas de incidencias.

En este subsistema se desarrolla las distintas consultas de incidencias registradas y se podrá generar estadísticas sobre estas.

- Consultas:
  - Por fechas
  - Por tipo de incidencia
  - Por estado de incidencia
  - Por responsable de resolución
- Estadísticas:
  - Contabilización de incidencias entre fechas
  - Contabilización de incidencias tipo

2.2. Identificación de actores.

Los actores que interviene en el procedimiento de registro de incidencias son usuarios registrados en el sistema, en el caso del usuario administrador tiene calidad de superusuario ya que se encarga de la gestión del resto de usuarios.

Administrador.-

Usuario del sistema cuya función es realizar el mantenimiento de usuarios del sistema, consiste en conceder, modificar o cancelar el acceso al sistema por parte de los usuarios y los distintos responsables.

Usuario:

Toda persona que tiene acceso a los datos de carácter personal de la base de datos del sistema de información, por tanto responsable de notificar cualquier incidencia que se produzca al responsable de seguridad.

Responsable Seguridad:

Usuario del sistema cuya función es gestionar las incidencias de seguridad. Recibe las notificaciones las incidencias de seguridad que afectan a datos de carácter personal, y lleva el control de la resolución. Se encargará de dar conocimiento al responsable del fichero para que tome las medidas oportunas para la resolución de la incidencia. Una vez resuelta la incidencia deberá cerrar la tramitación.

Responsable Recuperación

Usuario asignado por el responsable de seguridad de entre los usuarios con acceso al sistema, para que realice las labores de contención, evitar que el incidente siga produciéndose, eliminación del incidente y recuperación de los ficheros afectados. Recibe la comunicación de la incidencia para proceder a resolver la incidencia. Deberá comunicar al responsable de seguridad las actuaciones realizadas para la resolución de la incidencia.

2.3. Especificación de funcionalidades por subsistemas.

2.3.1. Subsistema de conexión y mantenimiento de usuarios.

Para acceder a la aplicación es necesario identificar se y autenticarse. La persona encargada del mantenimiento de usuarios autorizados es el administrador del sistema, este realiza la tareas de altas, modificaciones y bajas de usuario.

El perfil de administrador, estará creado previamente en el sistema con todas las autorizaciones de acceso al subsistema de conexión y mantenimiento.

El administrador creará el perfil a cada usuario, que determina para que operaciones está autorizado a realizar dentro del procedimiento.

Cuando el administrador dé de alta un usuario le asignará una contraseña, en la primera conexión que realice el usuario el sistema lo obligará a hacer un cambio de contraseña. También un usuario podrá cambiarse la contraseña cuando lo estime necesario o si cree que ha sido comprometida solicitándolo al administrador del sistema. Dispondremos de la fecha último cambio de contraseña, de esta manera podremos hacer caducar las contraseñas en un periodo como mínimo anual.

Cualquier usuario autenticado podrá ser asignado como responsable de recuperación, en el momento en que el responsable de seguridad le asigne la tarea de resolución de alguna incidencia. Este hecho capacita al responsable de seguridad para habilitar determinadas operaciones al usuario general.

Los datos referentes a cualquier actor que forme parte del sistema son:

- Nombre usuario
- Contraseña
- Dni
- Correo electrónico
- Departamento
- Perfil
- Fecha de alta
- Fecha modificación
- Fecha cambio contraseña
- Estado

2.3.2. Subsistema notificación y gestión de incidencia

En el proceso de notificación el actor implicado es el usuario que tiene acceso a los ficheros. Si el usuario detecta algún tipo de incidencia de seguridad tiene obligación de notificarlo al responsable de seguridad.

La notificación de la incidencia de seguridad debe contener la siguiente información para la posterior tramitación del procedimiento de gestión de la incidencia de seguridad:

- Tipo de incidencia
- Fecha y hora en que se produjo o detectó
- Persona que notifica la incidencia
- Categoría profesional de la persona comunicante.
- Persona a la que se notifica la incidencia
- Tipo de incidencia
- Causa de la incidencia

- Fichero afectados por la incidencia de seguridad
- Datos personales afectados
- Efectos derivados de la misma
- Recurso/s afectados

Posteriormente el sistema informará, al responsable de Seguridad, que se ha producido una incidencia de seguridad. El responsable de seguridad, una vez que ha recibido la incidencia y visto el detalle de la misma asignará al responsable de recuperación

.

El responsable de recuperación que se encargará de realizar las labores de contención, para que no continúe produciéndose la incidencia, eliminación, del problema que la ha ocasionado, y recuperación si fuera necesarios de los datos afectados o ficheros afectados.

Una vez resuelta la incidencia el responsable de la resolución deberá aportar al procedimiento la siguiente información sobre sus actuaciones:

- Identificación personal
- Recuperación de datos
- Procedimiento de recuperación
- Personas afectadas por la incidencia
- Efectos derivados de la incidencia
- Estado final
- Fecha de recuperación/solución

Terminado el procedimiento para solventar la incidencia, el responsable de la recuperación debe de realizar comunicación al responsable de seguridad, que se encargará de cerrar la incidencia, y en su caso, comunicarla a la AEPD.

2.3.3. Subsistema de consulta y estadísticas de incidencias.

Este subsistema será de gran utilidad para el control de seguridad por parte del responsable.

Aporta información muy valiosa que va a permitir desarrollar normas de uso y manipulación de los ficheros de carácter personal con objeto de evitar el mayor número posible de incidencias de seguridad.

2.4. Análisis y especificación de casos de uso.

2.4.1. Subsistema de conexión y mantenimiento.

Caso de Uso	Alta de usuario
Funcionalidad	Dar de alta un usuario en el sistema.
Actores	Administrador
Pre-condición	El usuario debe existir en el sistema y su estado debe ser alta
Pos-condición	El usuario cambia su estado a baja
Flujo	El administrador del sistema selecciona la opción alta usuario. El sistema muestra en pantalla los campos requeridos para crear usuario. El administrador introduce los datos requeridos. A continuación confirma los datos introducidos.
Excepciones	El usuario ya existe. Algunos datos introducidos del usuario coinciden con otro usuario existente en el sistema (dni,nombre usuario, clave de acceso). Campos obligatorios no introducidos.
Observaciones	El administrador establece el perfil que corresponde a cada usuario

Caso de Uso	Baja de usuario
Funcionalidad	Dar de baja un usuario de forma lógica, es decir cambiando el campo estado a

	situación de baja
Actores	Administrador
Pre-condición	El usuario debe existir en el sistema y su estado debe ser alta
Pos-condición	El usuario cambia su estado a baja
Flujo	El administrador del sistema selecciona la opción baja de usuario.
	El administrador introduce el nombre de usuario que va dar de baja.
	El sistema muestra los datos referentes al usuario
	El administrador introduce la fecha de baja y confirma la baja
Excepciones	El usuario no está creado en el sistema. El usuario está en estado baja.

Caso de Uso	**Modifica usuario**
Funcionalidad	Modificar algunos datos del usuario dado de alta en el sistema.
Actores	Administrador
Pre-condición	El usuario debe existir en el sistema y su estado debe ser alta
Pos-condición	Los datos del usuario quedan actualizados.
Flujo	El administrador del sistema selecciona la opción modifica usuario.
	El administrador introduce el nombre de usuario cuyos datos va a modificar.
	El sistema muestra los datos referentes al usuario
	El administrador modifica los datos y confirma la modificación
Excepciones	El usuario no está creado en el sistema. El usuario está en estado baja.

Caso de Uso	Conexión al sistema
Funcionalidad	Permite acceder al sistema mediante la identificación de los usuarios.
Actores	Administrador, Responsable de seguridad, usuario
Pre-condición	El usuario debe existir en el sistema y su estado debe ser alta
Pos-condición	Los datos introducidos para acceder son correctos y el usuario accede al sistema
Flujo	El sistema muestra al usuario la ventana de acceso. El usuario introduce nombre y contraseña El sistema comprueba que los datos son correctos El usuario accede al sistema.
.Excepciones	El nombre y contraseña son erróneos . El sistema permite introducir de nuevo el nombre y la contraseña.

Caso de Uso	Cambio de rol
Funcionalidad	Cambia el rol de usuario a responsable de recuperación y viceversa
Actores	Sistema
Pre-condición	El usuario debe existir en el sistema y su estado debe ser alta
Pos-condición	El usuario cambia su rol: Usuario- Responsable recuperación Responsable recuperación- Usuario
Flujo	El sistema recibe petición de cambio de rol, determinará qué cambio se realiza según sea Usuario o Responsable de

	recuperación

2.4.2. Subsistema de notificación y gestión de incidencia

Caso de Uso	**Alta comunicación de incidencia**
Funcionalidad	Comunicar que se ha producido una incidencia de seguridad que afecta a datos de carácter personal.
Actores	Usuario
Pre-condición	Se ha producido una incidencia de seguridad y el usuario ha accedido al sistema para notificarla
Pos-condición	La incidencia de seguridad ha sido dada de alta
Flujo	Este caso de inicia cuando un usuario del sistema detecta una incidencia de seguridad, selecciona la opción de notificar incidencia. El usuario introduce los datos requeridos para este trámite. Puede seleccionar un tipo de incidencia de la lista de incidencias y si existe insertar una nueva. El sistema valida los datos introducidos Confirmado el trámite, los datos quedan almacenados. El sistema avisa al responsable de seguridad de una nueva incidencia.
Excepciones.	Los datos son incorrectos entonces el sistema envía la pantalla de notificación indicando que datos son erróneos. El sistema permite realizar de nuevo la introducción de los datos.

Caso de Uso	**Petición: resolver incidencia**

Funcionalidad	El responsable de seguridad, recibida la notificación de la incidencia la analiza y realiza la petición de resolución de la incidencia, asignando a un usuario como responsable de recuperación.
Actores	Responsable de seguridad, responsable de recuperación (no primario).
Pre-condición	Se ha notificado una incidencia de seguridad
Pos-condición	Se ha asignado la resolución de la incidencia a un usuario responsable de recuperación
Flujo	Se inicia cuando el responsable de seguridad selecciona el trámite de petición resolver incidencia. Introduce los datos requeridos en el trámite principalmente seleccionará al usuario asignándolo como responsable de recuperación. Al confirmar la petición: - el sistema resolverá el rol del usuario pasando a ser usuario responsable. - el sistema avisa, al responsable de recuperación asignado, de la petición de resolución.

Caso de Uso	**Resolver incidencia**
Funcionalidad	El responsable de recuperación recibida la petición de resolución de la incidencia actuará para la contención eliminación y resolución de la incidencia. A continuación realiza la comunicación de las medidas adoptadas en la resolución

	de la incidencia.
Actores	Responsable de recuperación, responsable de seguridad (no primario).
Pre-condición	Se ha asignado la resolución de una incidencia de seguridad
Pos-condición	Se comunica la resolución de la incidencia al responsable de seguridad.
Flujo del trámite	Se inicia cuando el responsable de recuperación, una vez llevado a cabo las actuaciones pertinente para resolver la incidencia, procede a realizar el trámite de comunicación de las medidas adoptada, seleccionando esta opción. Introduce los datos relativos al resultado de la recuperación y actuaciones realizadas. Confirmado el trámite el sistema comunica al responsable de seguridad Al confirmar la petición: - el sistema resolverá el rol del usuario responsable pasando a ser usuario - el sistema comunica al responsable de seguridad la resolución de la petición.

Caso de Uso	**Cerrar incidencia**
Funcionalidad	El responsable de seguridad, recibe la comunicación de las actuaciones llevadas a cabo para la resolución de la incidencia. Dando el visto bueno y procede a cerrar la incidencia.
Actores	Responsable de seguridad
Pre-condición	Ha recibido comunicación de medidas adoptadas.
Pos-condición	Cerrar incidencia.
Flujo del trámite	El responsable de seguridad recibe

	comunicación de las medidas adoptadas. Comprueba las actuaciones realizadas. Verificada la resolución cierra la incidencia.
Observaciones	El responsable de seguridad si lo estima oportuna enviará comunicación AEPD

2.4.3. Subsistema de consulta y estadísticas de incidencias.

Caso de Uso	Consulta de incidencias por fechas
Funcionalidad	Permite consultar las incidencias producidas en entre dos fechas dadas.
Actores	Responsable seguridad
Pre-condición	Se ha seleccionado la consulta
Pos-condición	Se muestra la consulta
Flujo	El responsable de seguridad selecciona la opción de consulta de incidencias por responsable. Introduce el periodo entre fechas. El sistema muestra una lista de incidencias acaecidas entre las dos fechas dadas.
Excepciones	No existen incidencias entre las fechas introducidas por el responsable de seguridad. El sistema informa de este hecho y permite al responsable de seguridad introducir otro periodo de fechas.

Caso de Uso	Consulta por tipo incidencia
Funcionalidad	Permite consultar las incidencias producidas por tipo.
Actores	Responsable seguridad
Pre-condición	Se ha seleccionado la consulta
Pos-condición	Se muestra la consulta
Flujo	El responsable de seguridad selecciona la opción de consulta de incidencias por tipo de incidencia. El responsable de seguridad selecciona el tipo de incidencia de la lista de tipos. El sistema muestra una lista de

	incidencias del el tipo seleccionado.
Excepciones	No existen incidencias del tipo seleccionado. El sistema informa de este hecho y permite al responsable de seguridad seleccionar otro.

Caso de Uso	**Consulta por responsable resolución**
Funcionalidad	Permite conocer las incidencias que han sido asignadas a un usuario y en qué estado de la tramitación se encuentran.
Actores	Responsable de seguridad, responsable de recuperación, usuario
Pre-condición	El usuario seleccionado tiene incidencias asignadas, resueltas o no, por lo que en un momento del procedimiento de gestión ha sido asignado como responsable.
Pos-condición	Muestra nombre de responsable de resolución de incidencias, ordenadas por fecha y tipo de incidencia.
Flujo	El responsable de seguridad selecciona la opción de consulta de incidencias por responsable. El responsable de seguridad selecciona un usuario de entre los usuarios del sistema El sistema muestra una lista de incidencias con los datos de la consulta.
Excepciones	El usuario seleccionado no ha sido en ningún momento responsable de resolución de algún tipo de incidencia. El sistema informa de este hecho y permite al responsable seleccionar otro usuario.

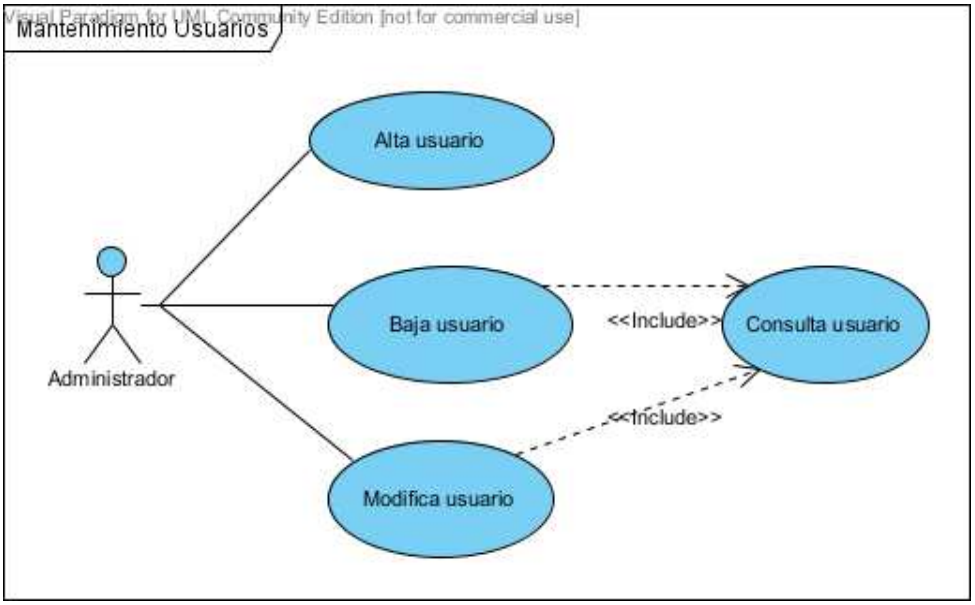
Caso de Uso	Consulta incidencias por estado
Funcionalidad	Permite conocer las incidencias seleccionadas según su estado: - Comunicada, - Asignada, - Resuelta, - Cerrada.
Actores	Responsable de seguridad
Pre-condición	Se ha seleccionado consulta de incidencias por estado y existen incidencias
Pos-condición	Muestra lista de incidencias por estado.
Flujo	El responsable de seguridad selecciona la opción consulta incidencias por estado. El responsable de seguridad selecciona el estado por el cual quiere consultar. El sistema muestra la lista de incidencias que están en el estado previamente seleccionado.
Excepciones	No hay incidencias en el estado que ha seleccionado el responsable de seguridad. El sistema informa del hecho y permite seleccionar otro estado,.

Caso de Uso	Informe estadístico anual
Funcionalidad	Mostrar un resumen estadístico de todas las incidencias producidos en un año natural.
Actores	Responsable de seguridad
Pre-condición	Ingresar en el sistema y seleccionar opción estadísticas
Pos-condición	Muestra informe anual
Flujo	El responsable de seguridad selecciona la opción de estadísticas.
	Selecciona ejercicio del cual quiere obtener el informe estadístico.
	El sistema muestra el informe
Execpciones	El ejercicio no es menor que el actual El sistema permite introducir otro ejercicio

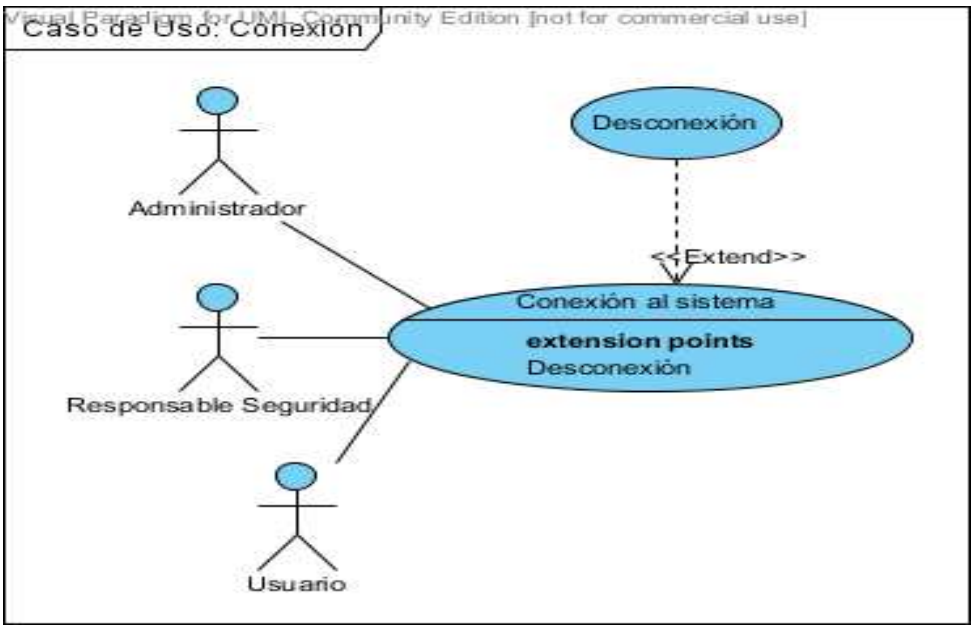
2.5. Diagramas de casos de uso.

2.5.1. Subsistema de conexión y mantenimiento de usuarios.

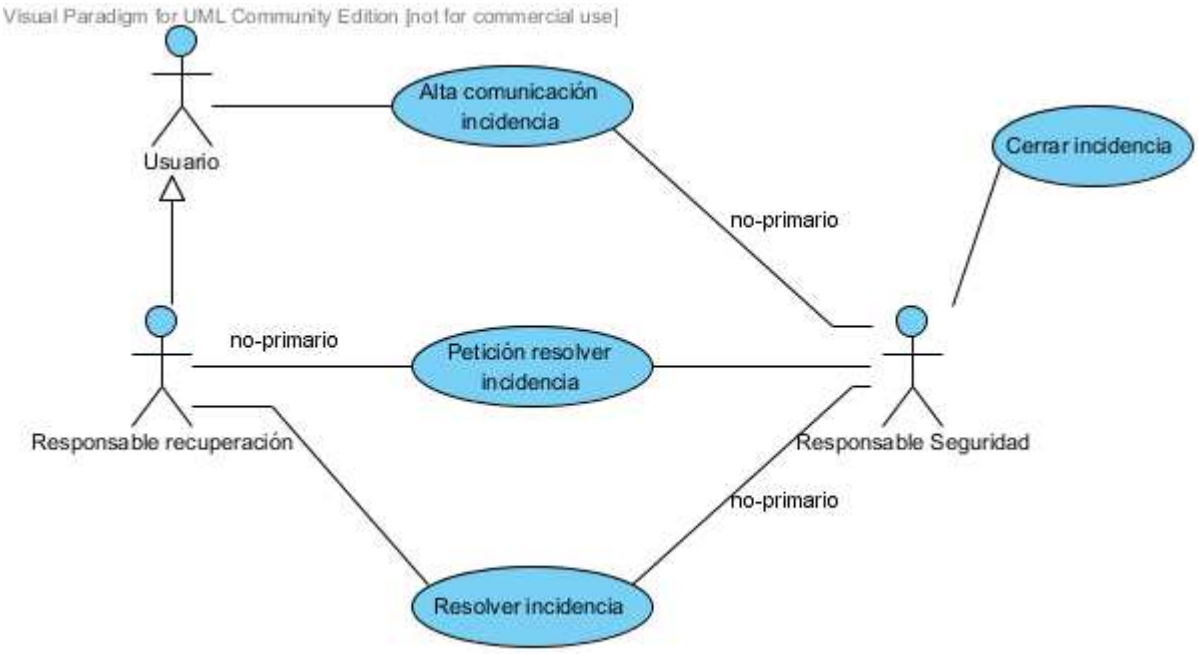
Mantenimiento de usuarios.



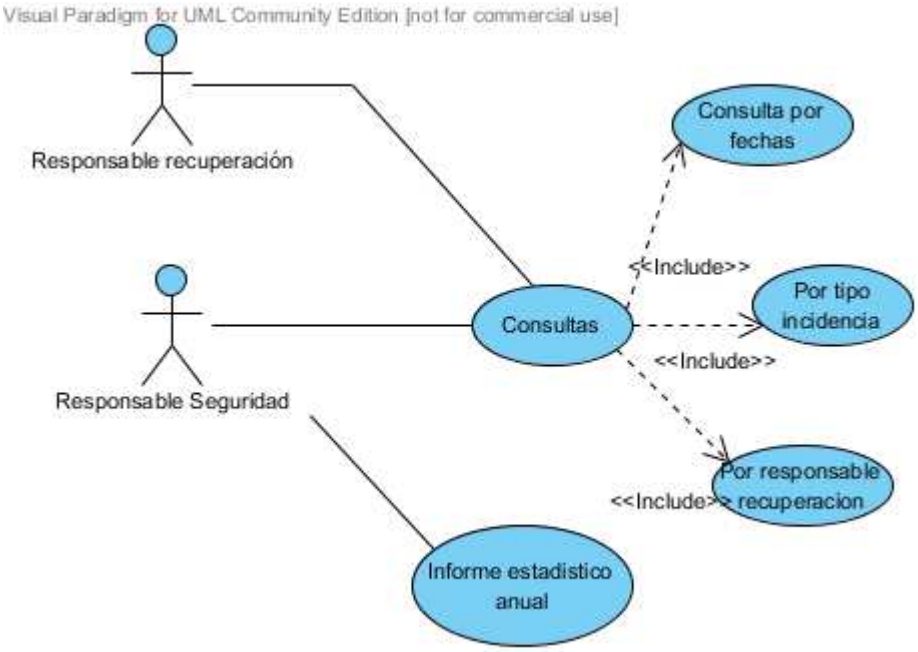
Conexión.



2.5.2. Subsistema notificación y gestión de incidencia


Visual Paradigm for UML Community Edition [not for commercial use]
Usuario
Alta comunicación incidencia
Cerrar incidencia
no-primario
no-primario
Petición resolver incidencia
Responsable recuperación
Responsable Seguridad
no-primario
Resolver incidencia

2.5.3. Subsistema de consulta y estadísticas de incidencias.



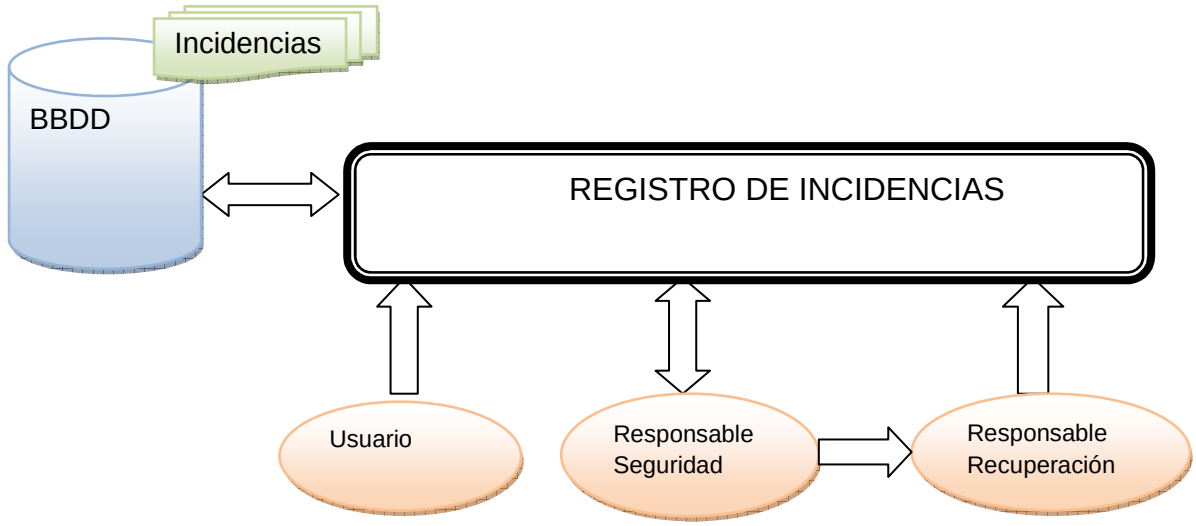
3. Diseño técnico.

3.1. Introducción.

La fase de diseño parte de las especificaciones desarrollada en la fase de análisis de requerimientos.

El diseño de los distintos subsistema se realiza teniendo en cuenta las interrelaciones que existen entre ellos.

La detección y registro de incidencias la realiza el usuario del sistema de información. El responsable de seguridad, a partir del registro de las incidencias, será el encargado del control del flujo que ha de seguir la incidencia hasta que esta quede resuelta, asignará a un responsable de recuperación, este se encarga de realizar el proceso necesario para solucionar la incidencia. Una vez que la incidencia queda solucionada, el responsable de recuperación deberá registrar el procedimiento seguido.



Se va a establecer la representación gráfica de los subsistemas y sus relaciones.

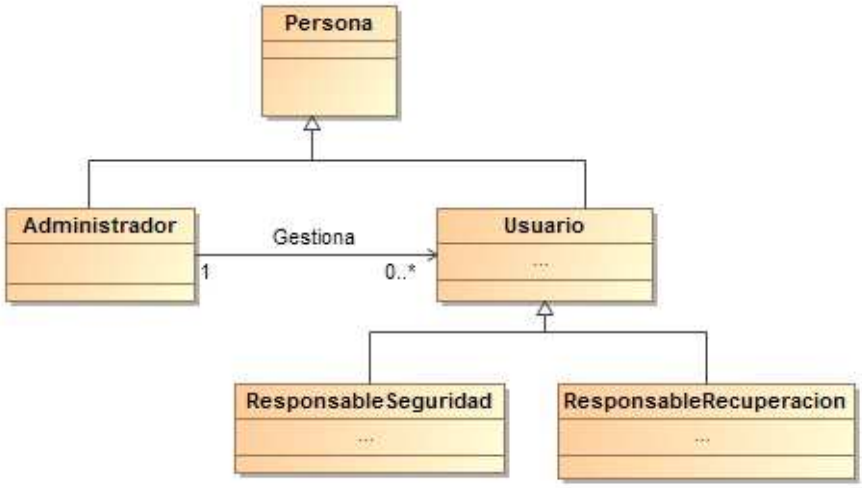
- Identificación de clases
- Diagramas de clases y jerarquías
- Diagramas de estados
- Diagramas de secuencia
- Diseño de la interfaz de usuario.

3.2. Identificación de clases.

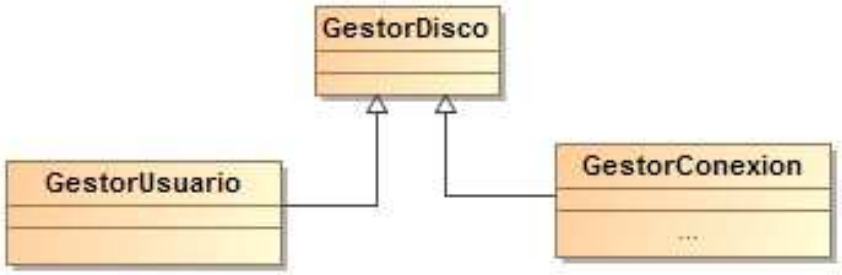
Subsistemas	Clases
Subsistema Conexión y Mantenimiento	
	Persona
	Usuario
	ResponsableSeguridad
	ResponsableRecuperacion
	Conexion
Subsistema Registro Incidencias	
	Incidencias
	Agsinar
	Recuperar
Subsistema Consulta Estadísticas	
	Estadisticas

3.2.1. Subsistema de conexión y mantenimiento.

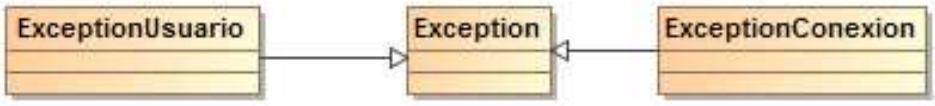
3.2.1.1. Diagrama de clases.



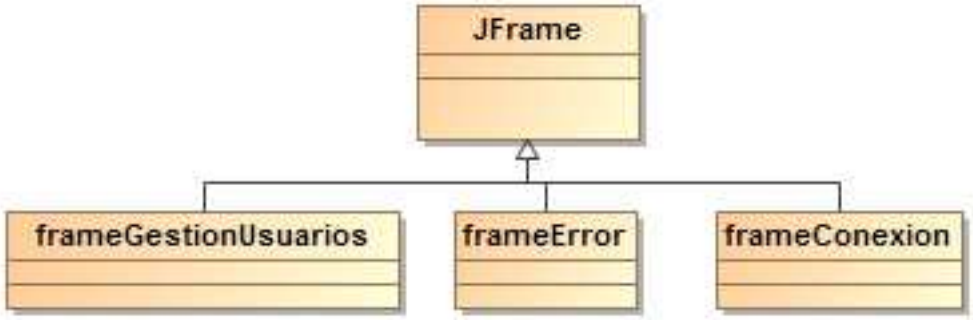
3.2.1.2. Diagrama de clases gestoras



3.2.1.3. Diagrama de excepciones.

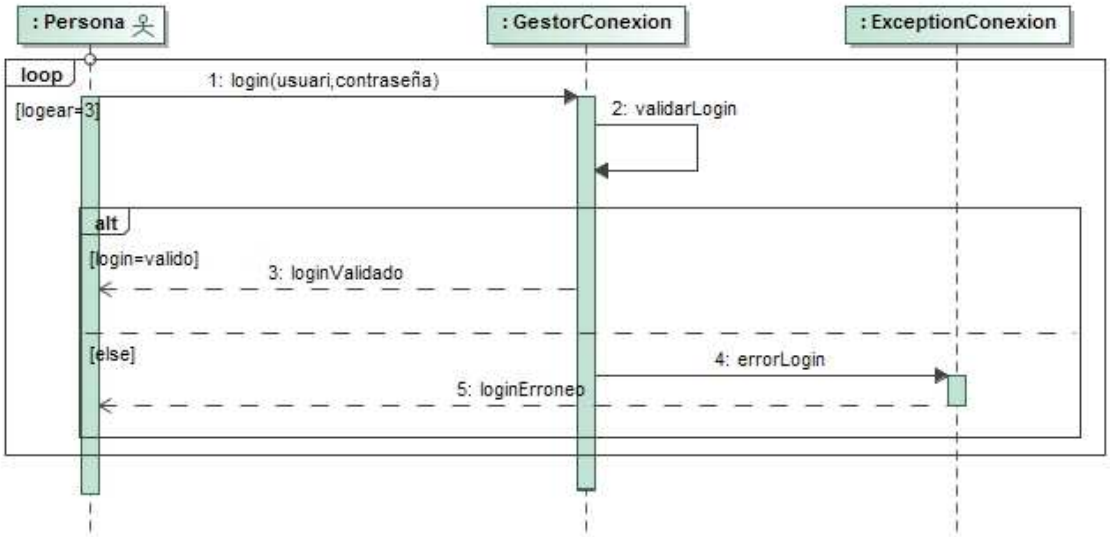


3.2.1.4. Diagrama clases frontera.



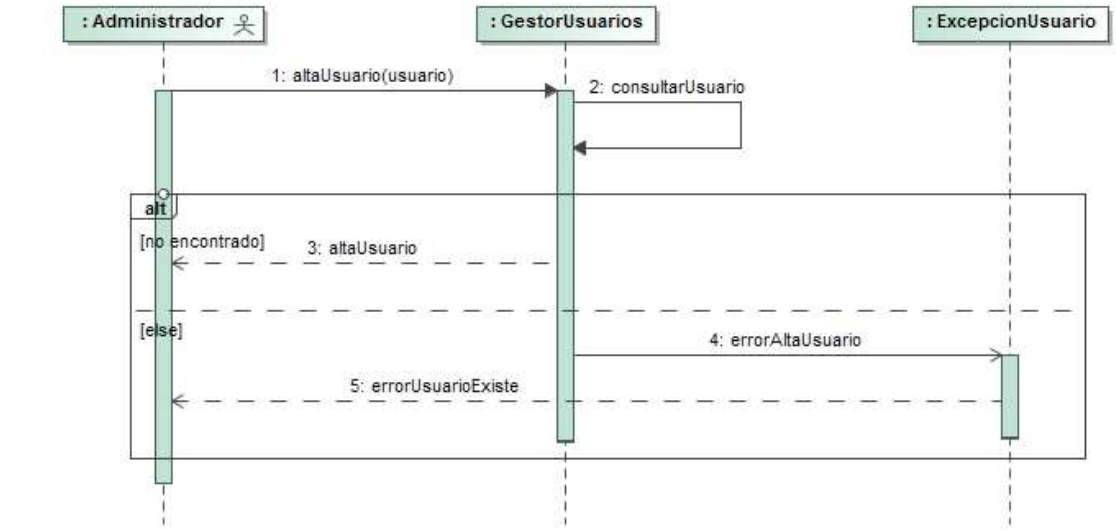
3.2.1.5. Diagrama de secuencia.

Gestor conexión

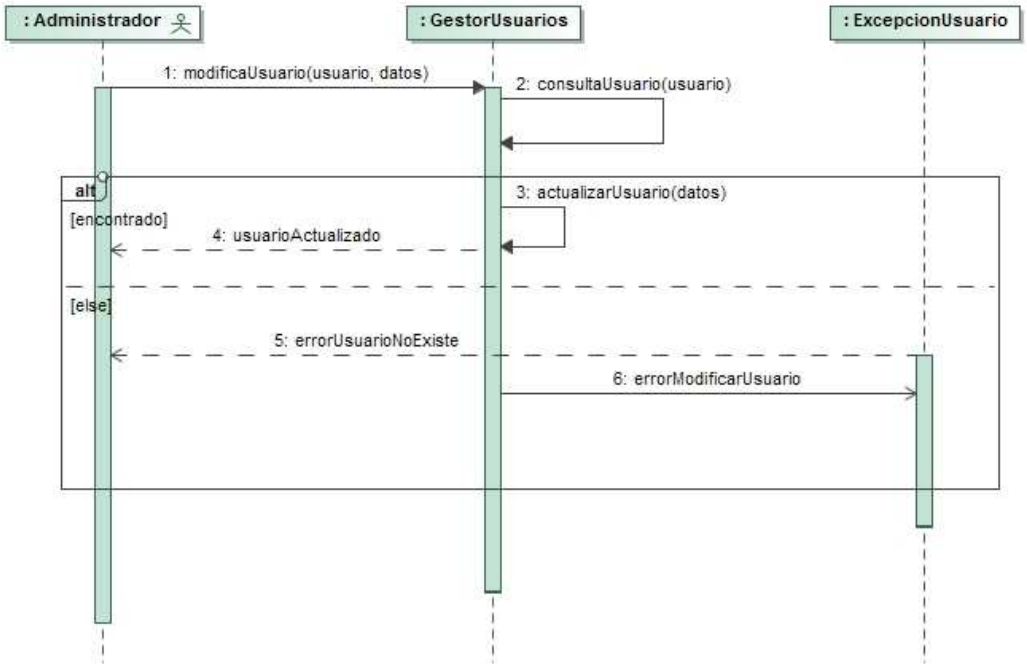


Gestor Usuarios: altas y modificaciones de usuarios. Las bajas se realiza modificando el estado del usuario.

Alta de Usuarios

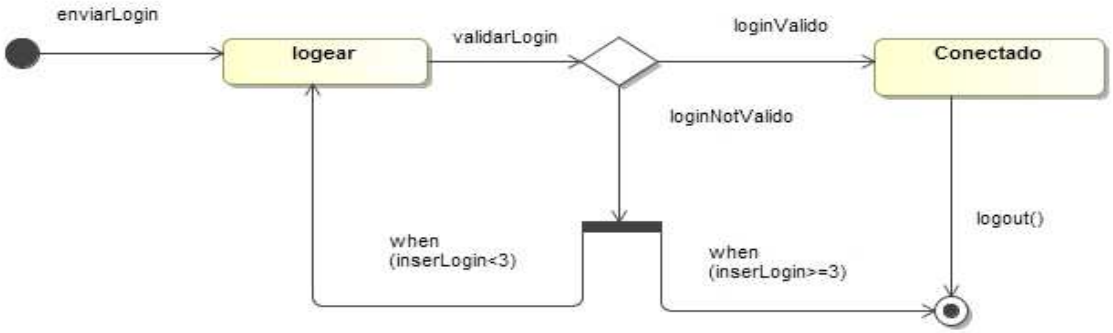


Modificar Usuarios

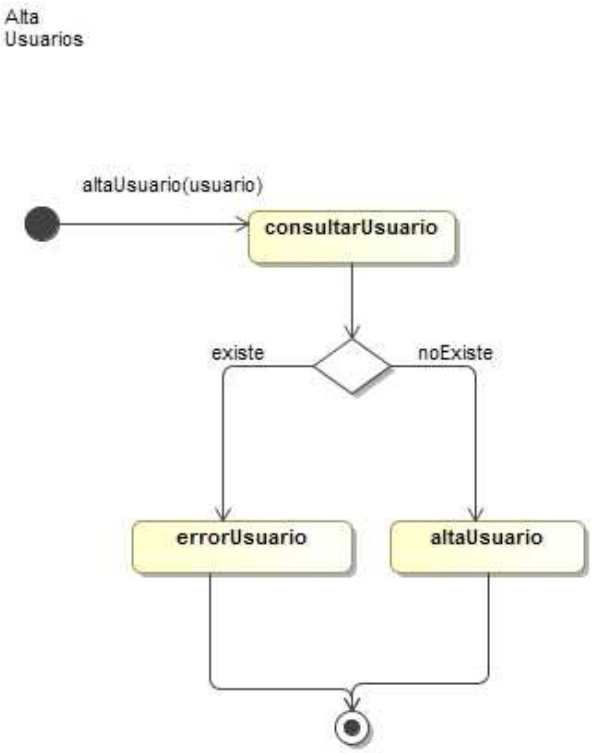


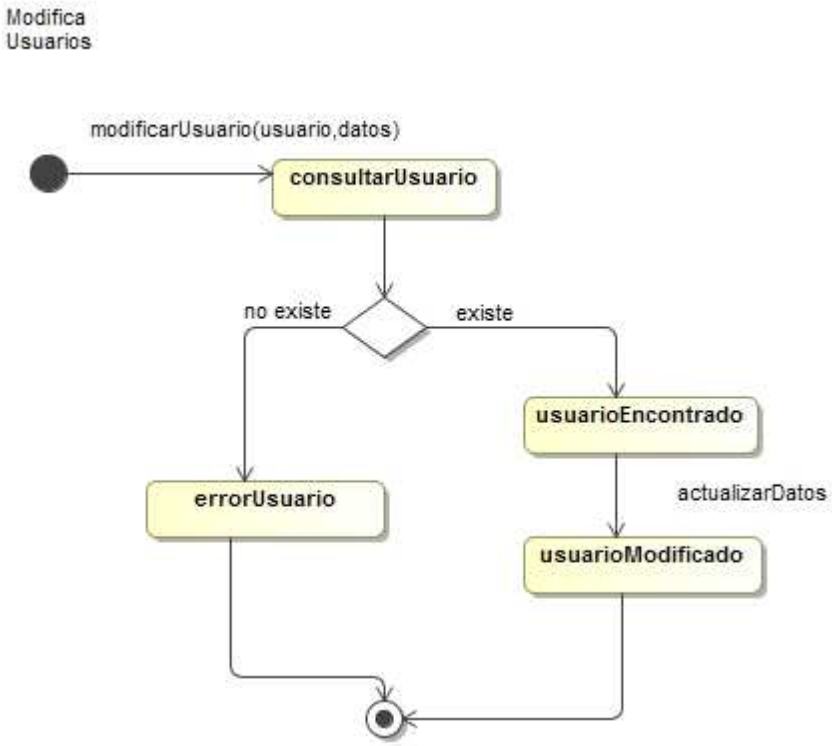
3.2.1.6. Diagrama de estado.

Gestor conexión



Gestor usuario





3.2.1.7. Notación CRC de clases.

Clase	Persona
Descripción	Define las propiedades comunes de toda persona que interviene en el sistema
Tipo	Clase principal
Responsabilidad	Modela un objeto persona con sus datos básicos.
Características	Abstracta, compuesta
Atributos	#idpersona:integer #nombre:string #apellidos:string #password:string #direccion:string #dni:string #estado:string #email:string #fechaAlta:date #fechaModificacion:date
Métodos	+Persona(idpersona:integer,nombre:string,apellidos:string,password:string, direccion:string,dni:string,estado:string,email:string,fechaAlta:date, fechaModificacion:date)

+getNombre():string
+setNombre(nombre:string)
+getApellidos():string
+setApellidos(apellidos:string)
+getDireccion():string
+setDireccion(direccion:string)
+getDni():string
+setDni(dni:string)
+getEstado():string
+setEstado(estado:string)
+getEmail():string
+setEmail(email:string)

Clase	Administrador
Descripción	Hereda de persona, administrador del sistema
Tipo	Clase principal
Responsabilidad	Modela un objeto administrador .
Características	Concreta, compuesta, persistente
Atributos	#idAdministrador:integer
Métodos	+Administrador(idAdministrador:integer,nombre:string,apellidos:string, password:string,direccion:string,dni:string,estado:string,email:string, fechaAlta:date, fechaModificacion:date) +altaUsuario(usuario) +modificarUsuario(usuario) +buscaUsuarioNombre(nombre:string):usuario +buscaUsuarioDni(dni:string):usuario +consultaUsuarios(nombre:String):List<usuarios<

Clase	ResponsableSeguridad
Descripción	Especificación de la clase usuario
Tipo	Clase principal
Responsabilidad	Modela un objeto responsable de seguridad.
Características	Concreta, compuesta, persistente
Atributos	#idRSeguridad:integer
Métodos	+responsableSeguriad(idRSeguridad:integer,nombre:string,apellidos:string, password:string,direccion:string,dni:string,estado:string,email:string, fechaAlta:date, fechaModificacion:date)

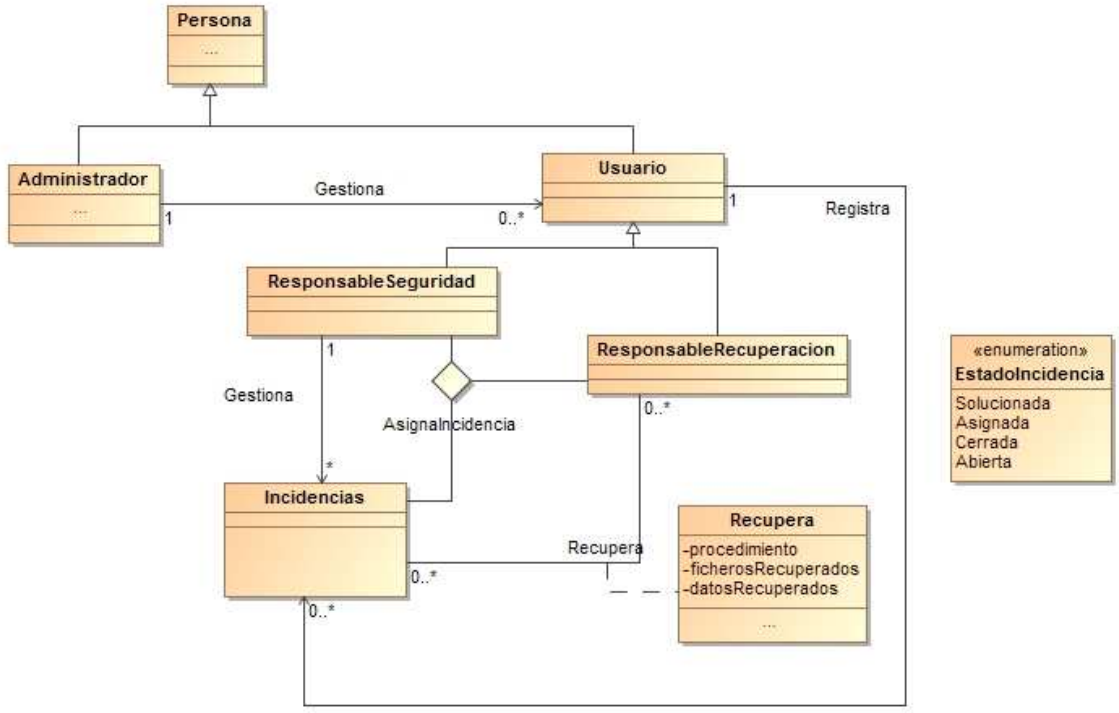
Clase	Usuario
Descripción	Hereda de persona
Tipo	Clase principal
Responsabilidad	Modela un objeto usuario.
Características	Concreta, compuesta, persistente
Atributos	#idUsuario:integer #puesto:String #responsabilidad:String
Métodos	+Usuario(idUsuario:integer,nombre:string,apellidos:string, password:string,direccion:string,dni:string,estado:string,email:string, fechaAlta:date, fechaModificacion:date) +getPuesto():String +setPuesto(puesto:String) +getResponsabilidad():String +setResponsabilidad(responsabilidad:string)

Clase	ResponsableRecuperacion
Descripción	Especificación de la clase usuario
Tipo	Clase principal
Responsabilidad	Modela un objeto responsable de recuperación.
Características	Concreta, compuesta, persistente
Atributos	#idResponsableR:integer
Métodos	+ResponsableR(idResponsableR:integer,nombre:string,apellidos:string, password:string,direccion:string,dni:string,estado:string,email:string, fechaAlta:date, fechaModificacion:date)

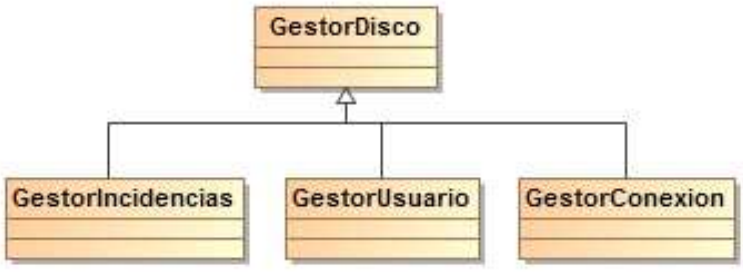
Clase	GestorUsuarior
Descripción	Implementa las operaciones básicas de gestión de usuarios
Tipo	Clase principal
Responsabilidad	Modela un objeto administrador .
Características	Concreta, compuesta, persistente
Atributos	#conexion
Métodos	+altaUsuario(usuario) +modificarUsuario(usuario) +buscaUsuarioNombre(nombre:string):usuario +buscaUsuarioDni(dni:string):usuario +listaUsuarios (usuario):List<usuarios>

3.2.2. Subsistema de registro de incidencias.

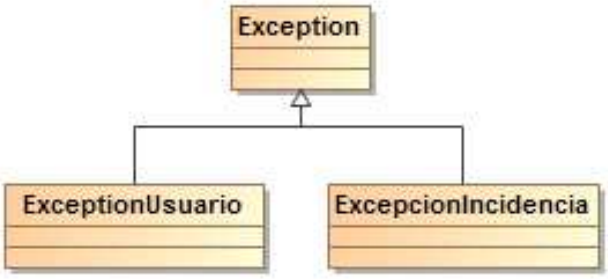
3.2.2.1. Diagrama de clases



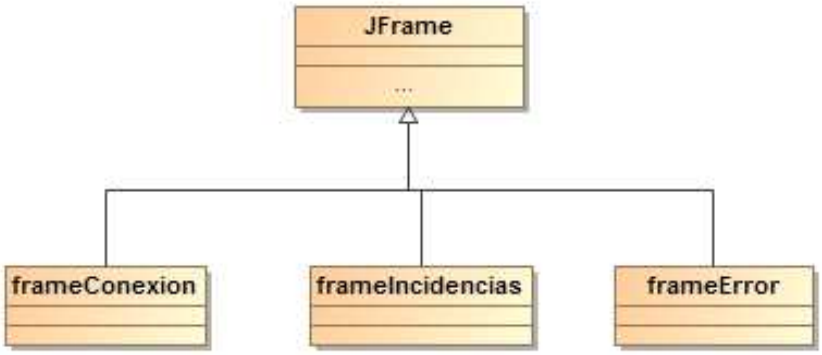
3.2.2.2. Diagrama de clases gestoras.



3.2.2.3. Diagrama de excepciones.

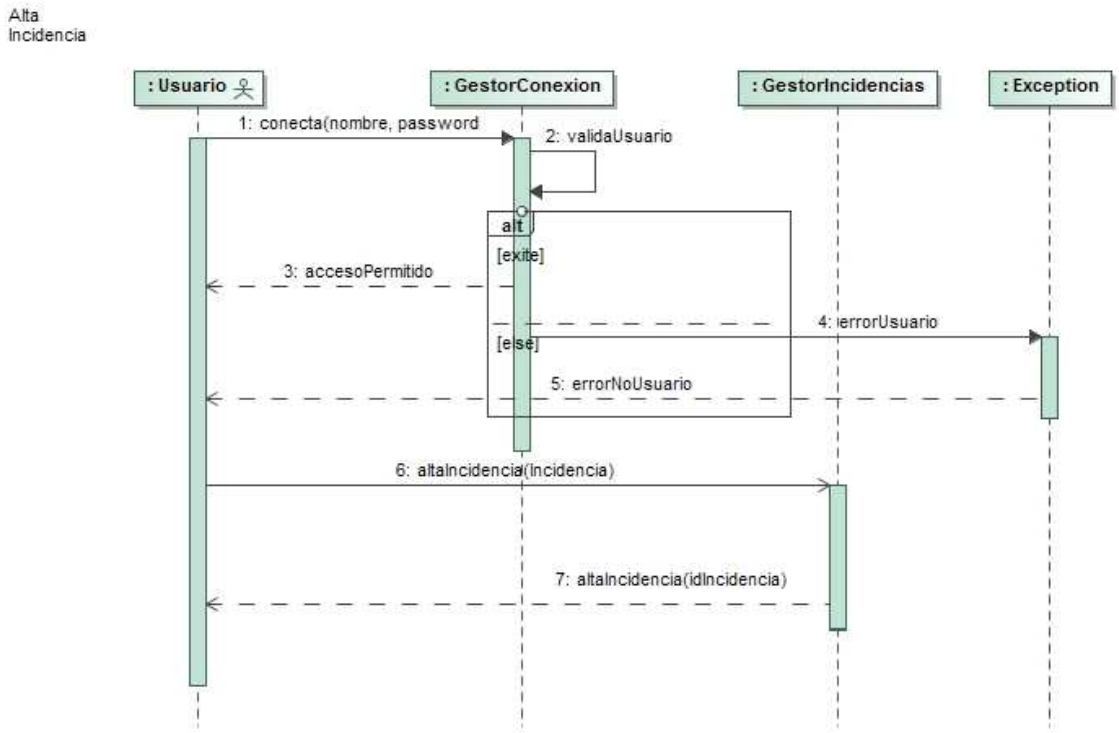


3.2.2.4. Diagrama clases frontera.

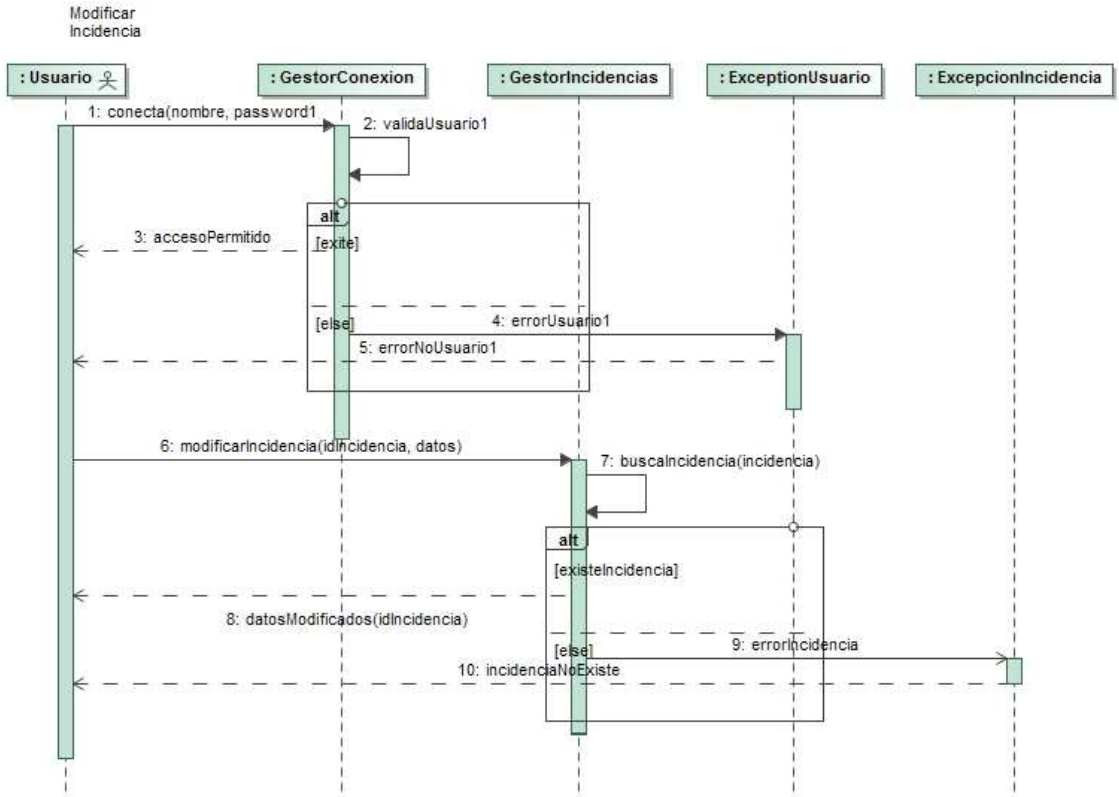


3.2.2.5. Diagrama de secuencia.

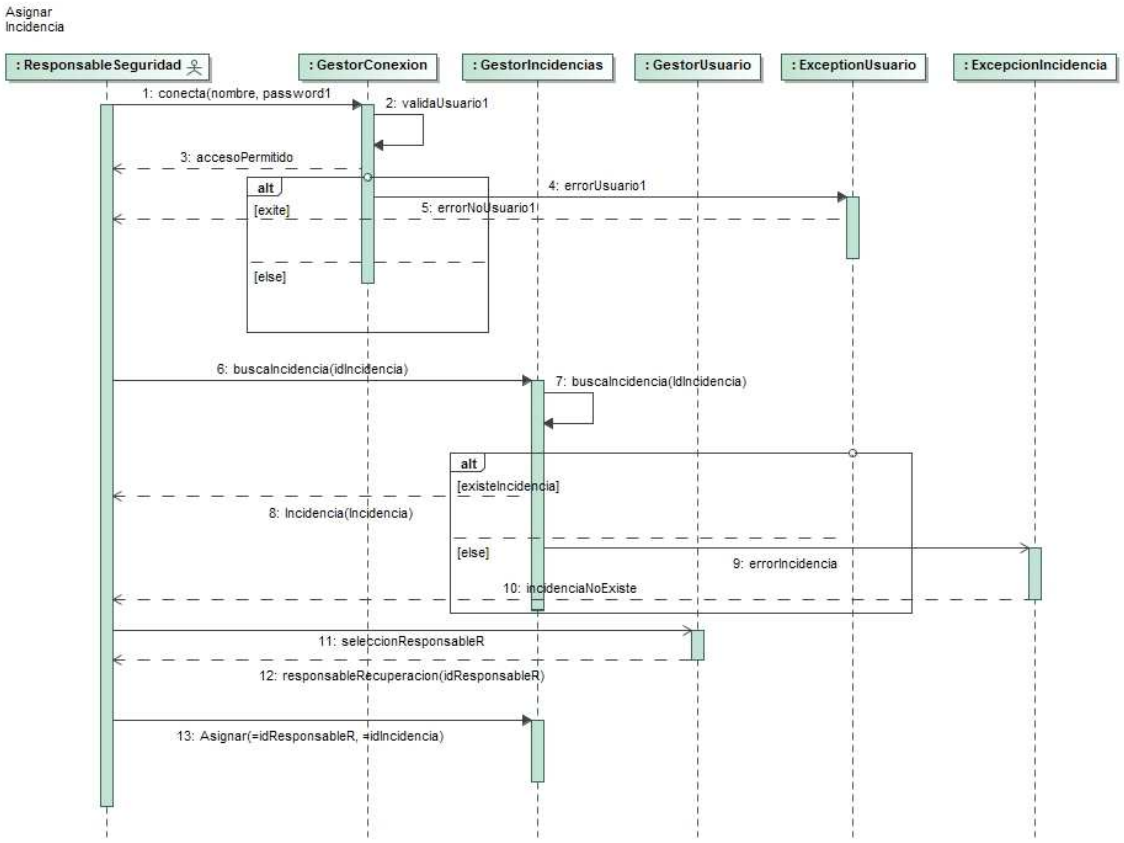
El proceso de alta de incidencia la realiza cualquier usuario que detecte cualquier tipo de incidencia que afecte a fichero que contenga datos personales.



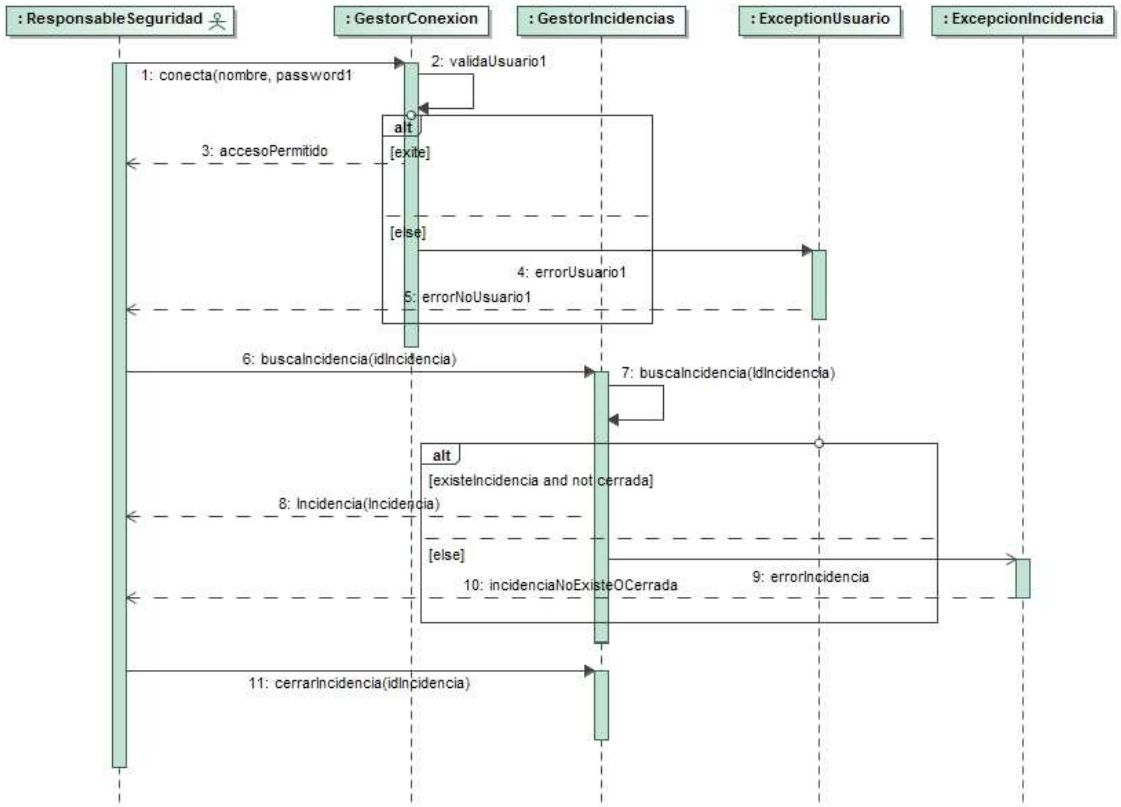
El usuario que ha realizado el alta de incidencia podrá realizar modificaciones sobre la misma.



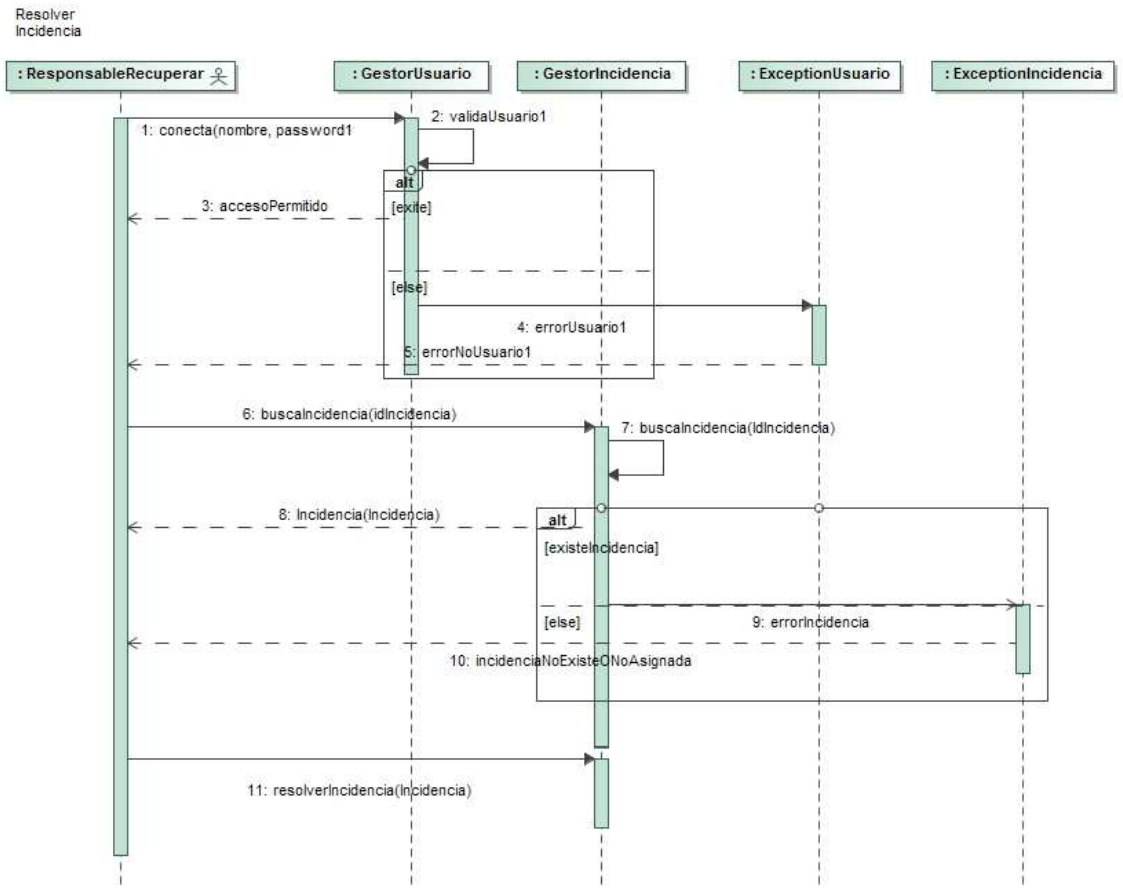
El responsable de seguridad se ocupará de asignar las incidencias que han dado de alta los distintos usuarios.



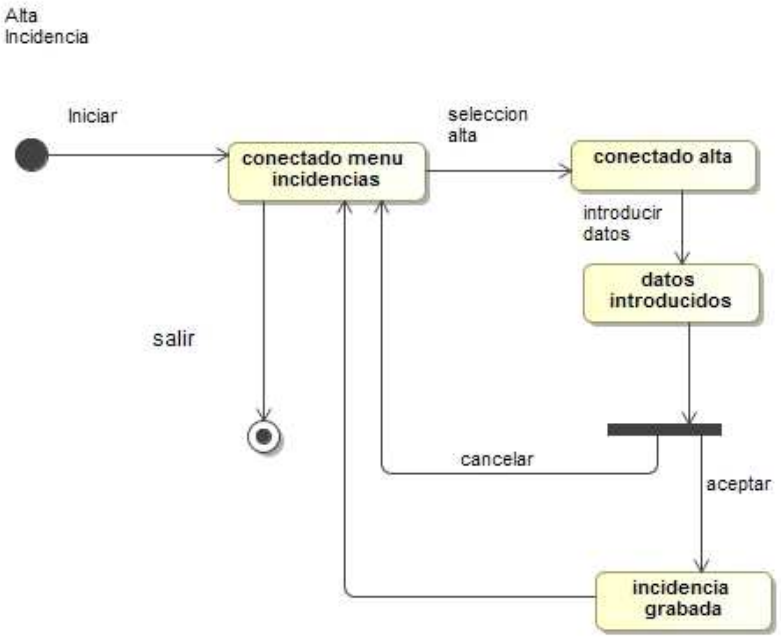
El responsable de seguridad, una vez se han realizado los procedimientos para resolver las incidencias, realizará el cierre de las mismas.

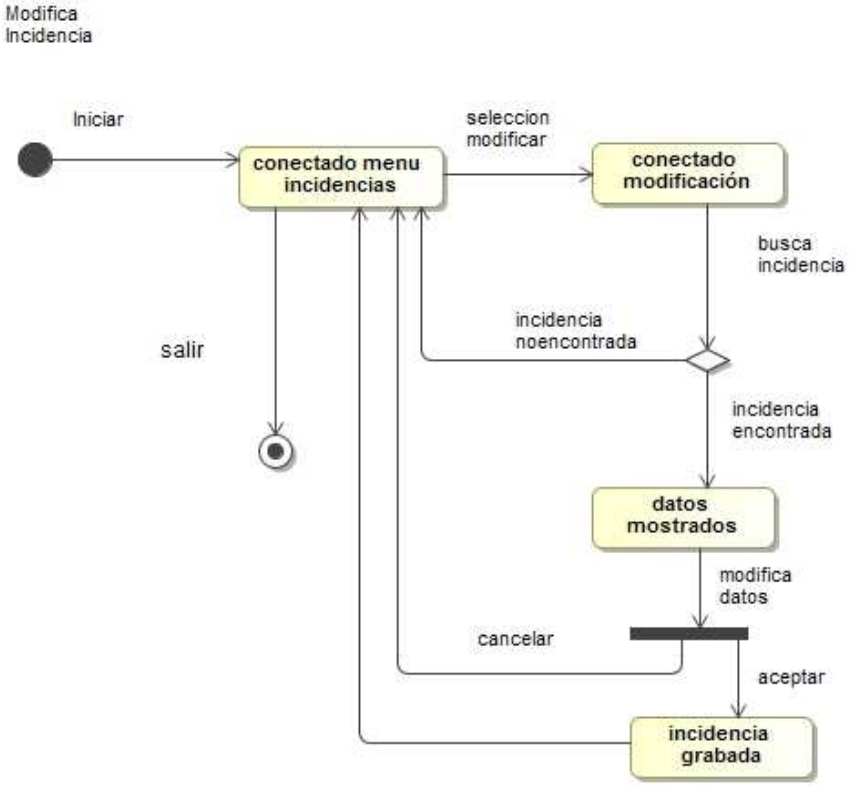


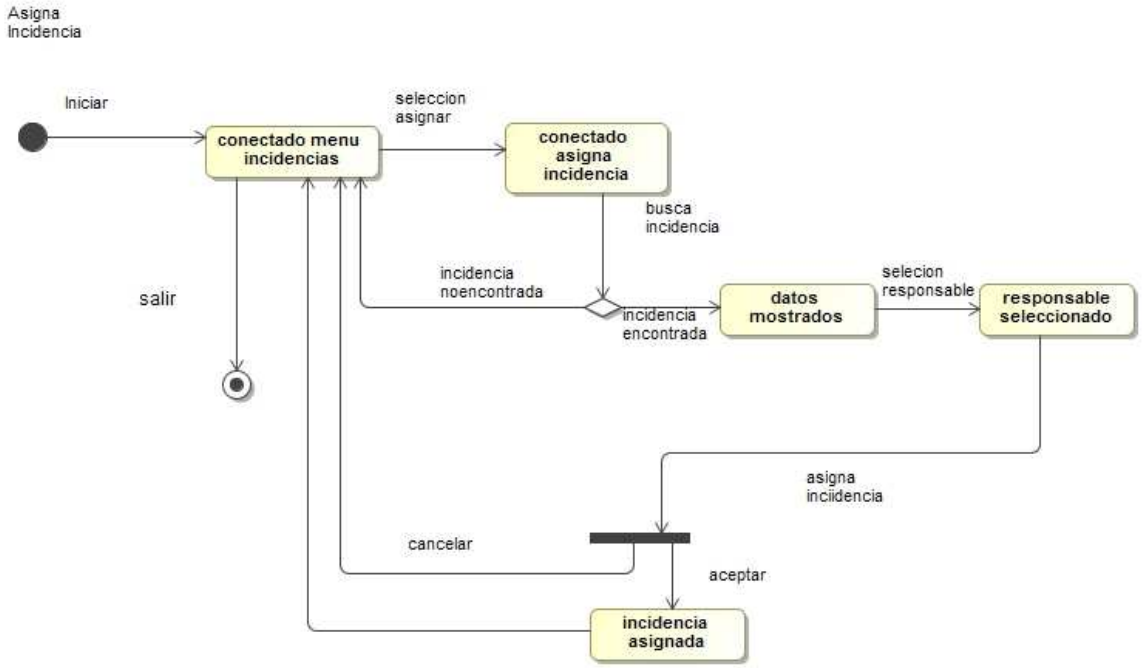
El responsable de resolución de incidencias procederá a realizar los procedimientos adecuados para solventar las incidencias que le han sido asignadas.

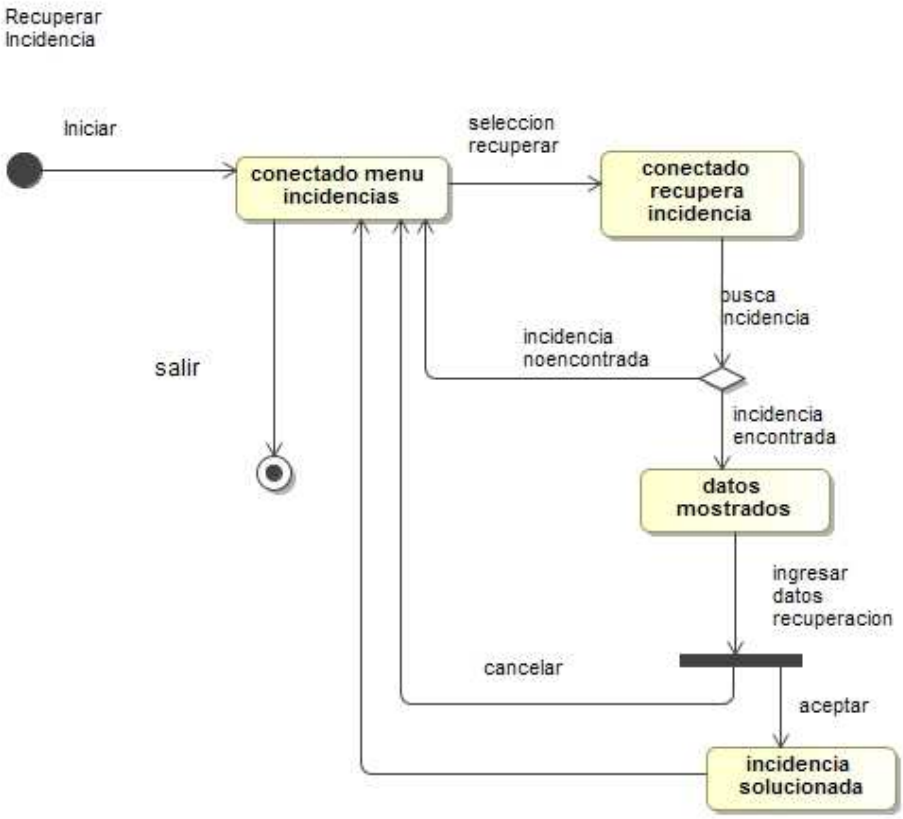


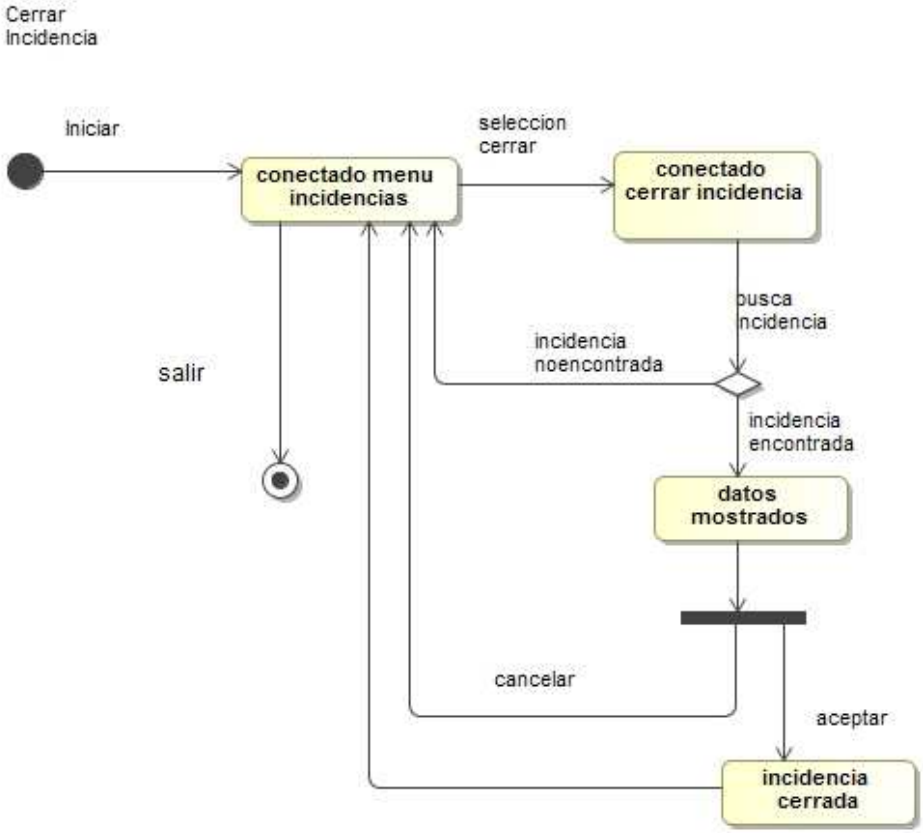
3.2.2.6. Diagrama de estados.






Asigna
Incidencia
Iniciar
conectado menu incidencias
seleccion asignar
conectado asigna incidencia
busca incidencia
incidencia noencontrada
incidencia encontrada
datos mostrados
selecion responsable
responsable seleccionado
salir
asigna inciidencia
cancelar
aceptar
incidencia asignada


Recuperar
Incidencia
Iniciar
conectado menu incidencias
seleccion recuperar
conectado recupera incidencia
busca incidencia
incidencia noencontrada
incidencia encontrada
datos mostrados
salir
ingresar datos recuperacion
cancelar
aceptar
incidencia solucionada


Cerrar
Incidencia
Iniciar
conectado menu
incidencias
seleccion
cerrar
conectado
cerrar incidencia
busca
incidencia
incidencia
noencontrada
salir
incidencia
encontrada
datos
mostrados
cancelar
aceptar
incidencia
cerrada

3.2.2.7. Notación CRC de clases.

Clase	Incidencia
Descripción	Describe la incidencia, recoge todas la propiedades
Tipo	Clase principal
Responsabilidad	Modela un objeto incidencia con sus datos
Características	Abstracta, compuesta
Atributos	#idIncidencia:integer #tipoIncidencia:String #nombreUsuario:string #descripcionIncidencia:string #ficheroAfectado:string #efectoIncidencia:String #fechaIncidencia:date #horaIncidencia:float #estadoIncidencia:string
Métodos	+Incidencia(idIncidencia:integer,tipoIncidencia:String,nombreUsuario:string ,descripcionIncidencia:string,ficheroAfectado:string,efectoIncidencia:String fechaIncidencia:date,horaIncidencia:float,estadoIncidencia:string) +getIdIncidencia():integer +setIdIncidencia(idIncidencia:integer) +getTipoIncidencia():string +setTipoIncidencia(tipoIncidencia:string +getNombreUsuario():string +setNombreUsuario(nombreUsuario:string) +getDescripcionIncidencia():string +setDescripcionIncidencia(descripcionIncidencia:string) +getFicheroAfectado():string +setFicheroAfectado(ficheroAfectado:string) +getEfectoIncidencia():string +setEfectoIncidencia(efectoIncidencia:string) +getFechaIncidencia():date +setFechaIncidencia(fechaIncidencia:date) +getHoraIncidencia():time +setHoraIncidencia(horaIncidencia:time) +getEstadoIncidencia():String

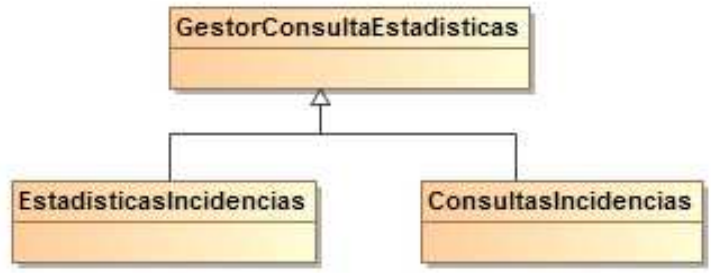
+setEstadoIncidencia(estadoIncidencia:String)

Enumeration	EstadoIncidencia
Descripción	Describe la relación de estados en los que se encuentra la incidencia
Tipo	Clase enumeration
Responsabilidad	Propiedad de la incidencia
Características	Atributos de clase

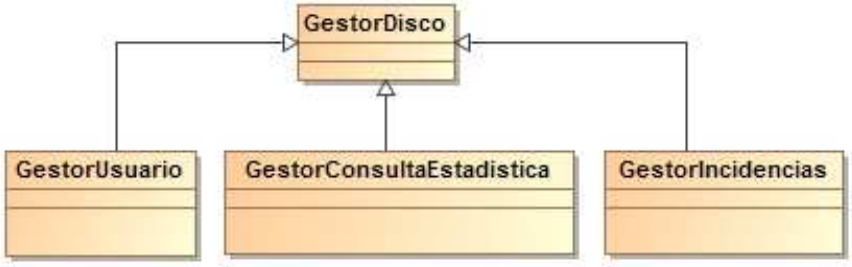
Clase	Recupera
Descripción	Describe el procedimiento seguido para solucionar la incidencia
Tipo	Clase asociada
Responsabilidad	Modela un objeto con las propiedades de la recuperacion
Características	Concreta
Atributos	#idRecupera:integern #procedimiento:String #datosRecuperados:string #ficherosRecuperados:string
Métodos	+Recupera(idRecupera:integer,procedimiento:String,datosAfectados:string ficherosAfectados:string) +getIdRecupera():integer +setIdRecupera(idRecupera:integer) +getProcedimiento():string +setProcedimiento(tipoIncidencia:string +getDatosRecuperados():string +setDatosRecuperados(datosRecuperados:string) +getFicherosRecuperados():string +setFicherosRecuperados(ficherosRecuperados:string)

3.2.3. Subsistema de consulta y estadísticas de incidencias.

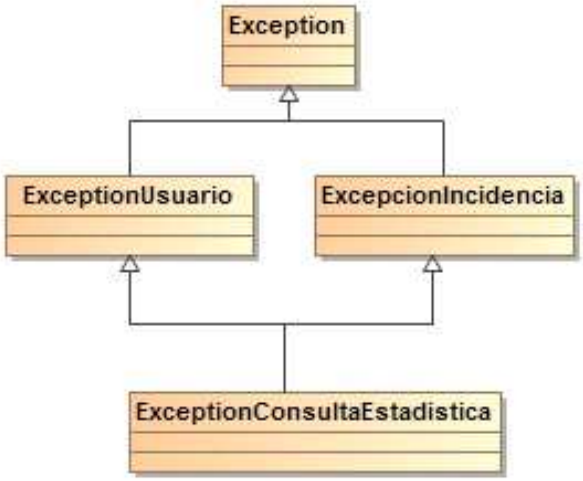
3.2.3.1. Diagrama de clases



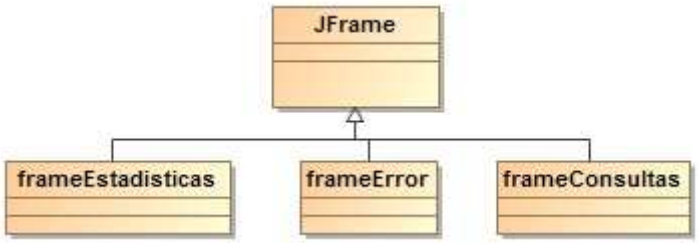
3.2.3.2. Diagrama de clases gestoras.



3.2.3.3. Diagrama de excepciones.

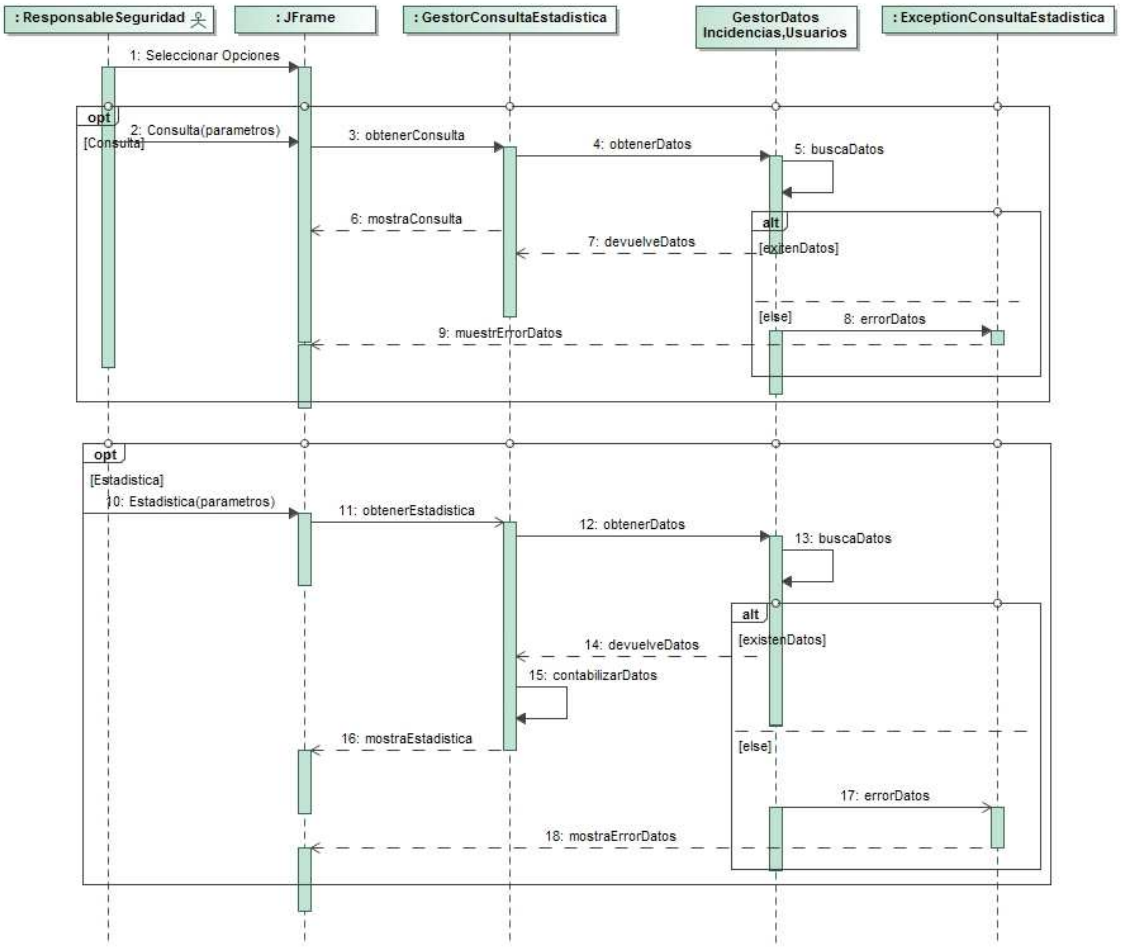


3.2.3.4. Diagrama clases frontera.



3.2.3.5. Diagrama de secuencia.

Gestor consulta y estadísticas: representamos de forma genérica el proceso que sigue la consulta y la obtención de estadística de incidencias.



3.2.3.6. Notación CRC de clases.

Clase	GestorEstadisticasConsultas
Descripción	Define los m propiedades comunes de toda persona que interviene en el sistema
Tipo	Iteración
Responsabilidad	Implementa operaciones para consulta y estadística de incidencias
Características	Abstracta, compuesta Colaboraciones: gestor usuarios, gestor incidencias
Atributos	
Métodos	+GestorConsultasEstadisticas() +listaIncidenciasEstado(estado:string):List<Incidencias +ConsultaIncidenciasFecha(fechaDesde:date,fechaHasta:date):List<Incidencias> +ConsultaIncidenciasAsignadas(idResponsableR:string):List<Incidencias> +getIncidenciaPorFecha(fecha:date): List<Incidencias> + listaIncidencias():List<Incidencias> +

3.3. Interfaz de usuario.

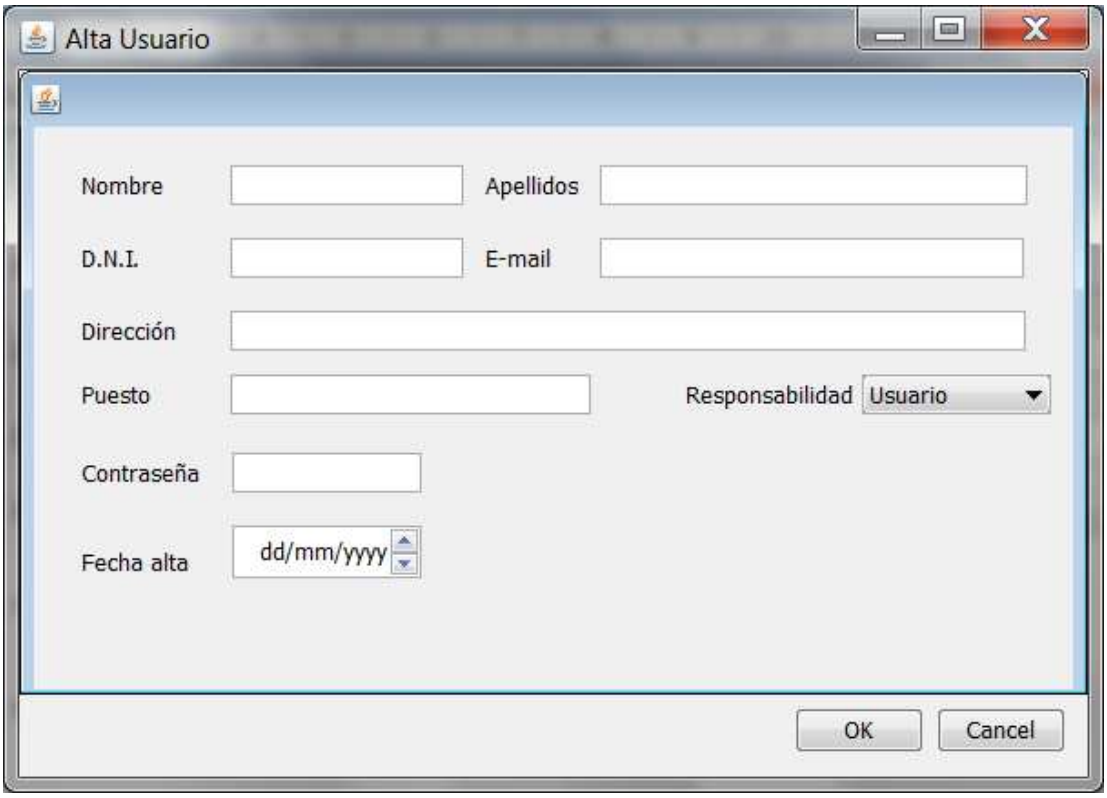
La pantalla de presentación del sistema de Registro de Incidencias, dispone de una barra menú de opciones disponibles. Cada una de estas opciones está compuesta por un menú desplegable que contiene las operaciones que se pueden realizar..

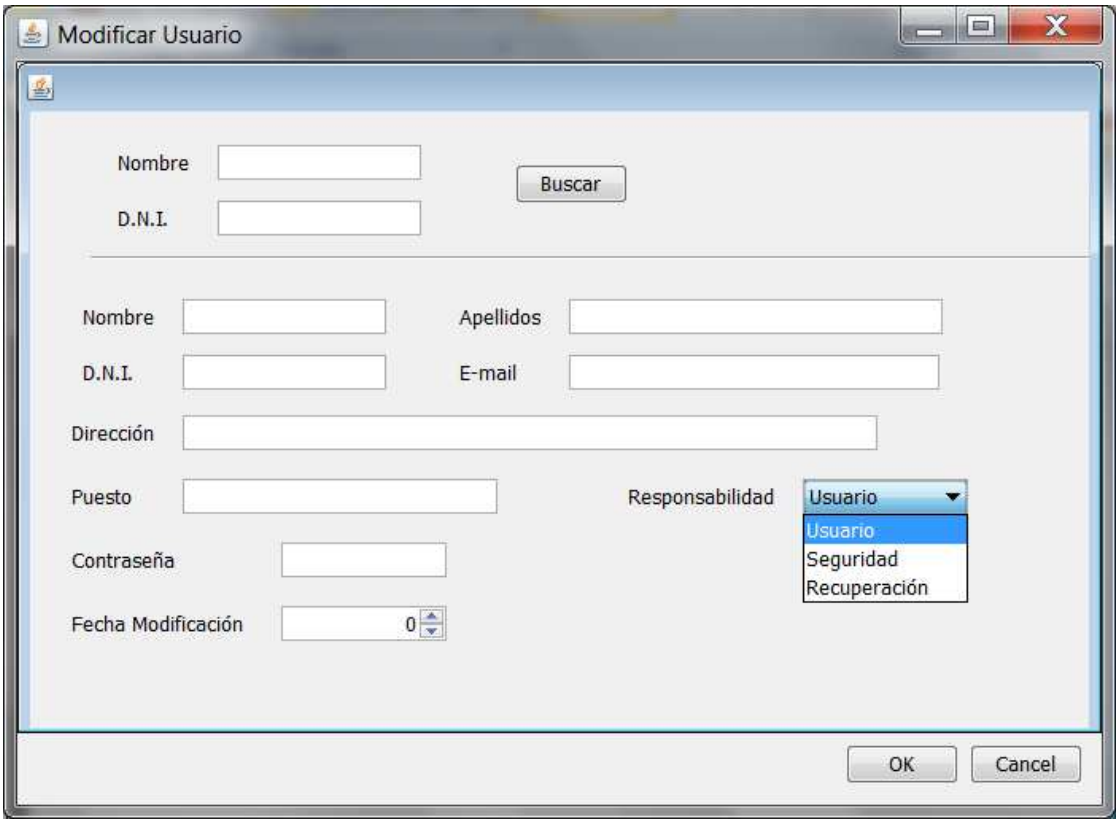
3.3.1. Subsistema de conexión y mantenimiento.

Desde el menú desplegable “Inicio” los distintos usuarios podrá introducir sus credenciales para el acceso al sistema de Registro de Incidencias.

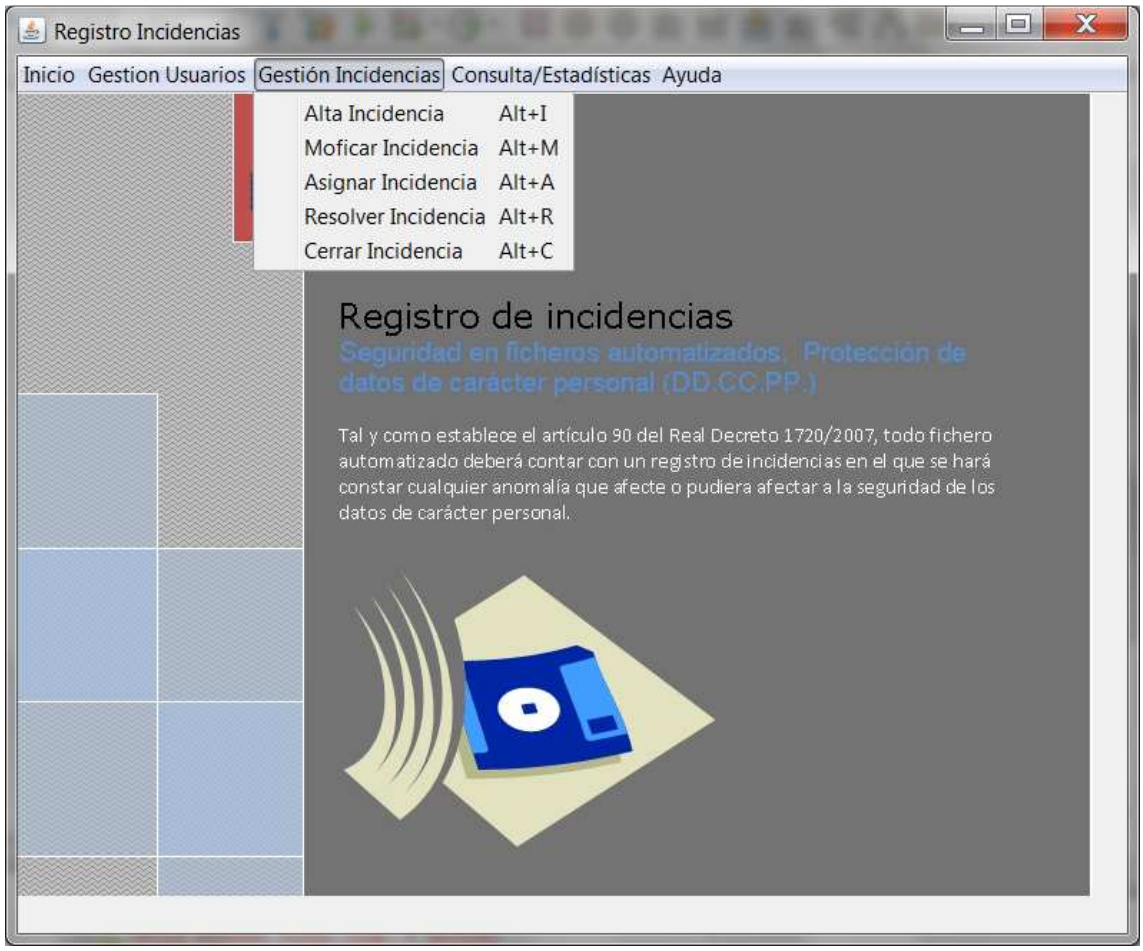
Pantalla donde el usuario del sistema introducirá sus credenciales para poder acceder.


Registro Incidencias
Inicio
Gestion Usuarios
Gestión Incidencias
Consulta/Estadísticas
Ayuda
Alta Alt+A
Modificación Alt+M
UOC
Registro de incidencias
Seguridad en ficheros automatizados. Protección de datos de carácter personal (DD.CC.PP.)
Tal y como establece el artículo 90 del Real Decreto 1720/2007, todo fichero automatizado deberá contar con un registro de incidencias en el que se hará constar cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos de carácter personal.

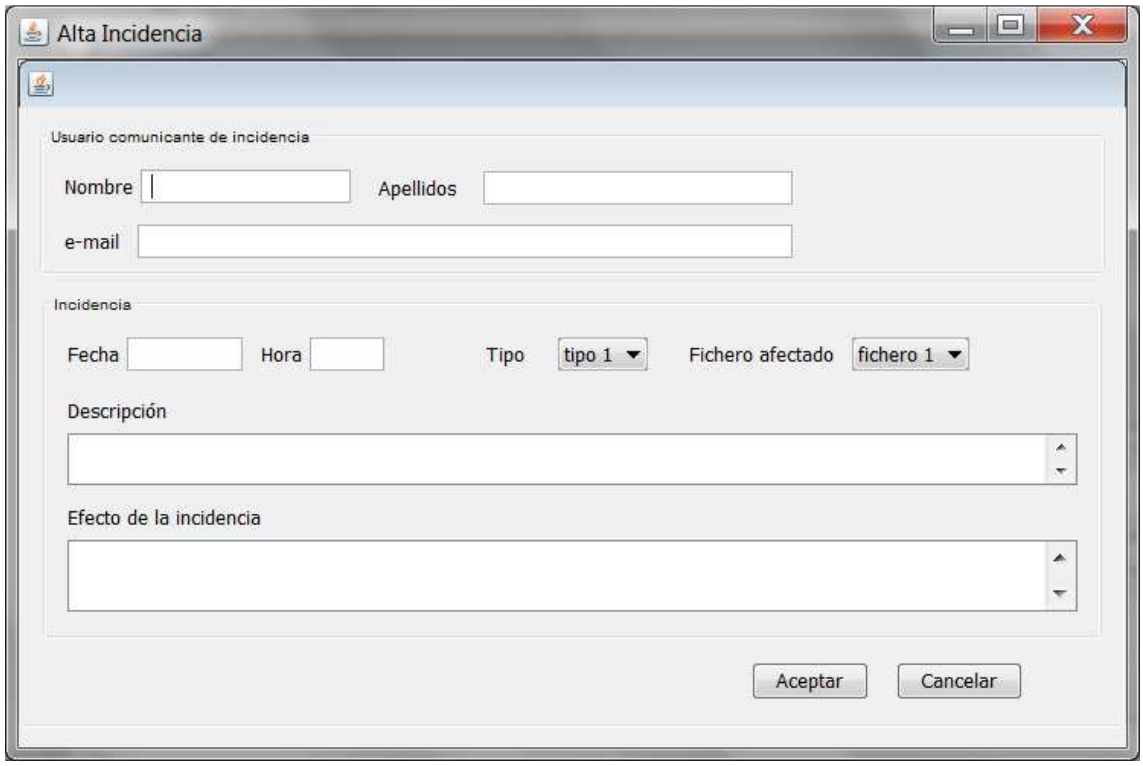

Alta Usuario
Nombre
Apellidos
D.N.I.
E-mail
Dirección
Puesto
Responsabilidad
Usuario
Contraseña
Fecha alta
dd/mm/yyyy
OK
Cancel


Modificar Usuario
Nombre
Buscar
D.N.I.
Nombre
Apellidos
D.N.I.
E-mail
Dirección
Puesto
Responsabilidad
Usuario
Usuario
Seguridad
Recuperación
Contraseña
Fecha Modificación
0
OK
Cancel

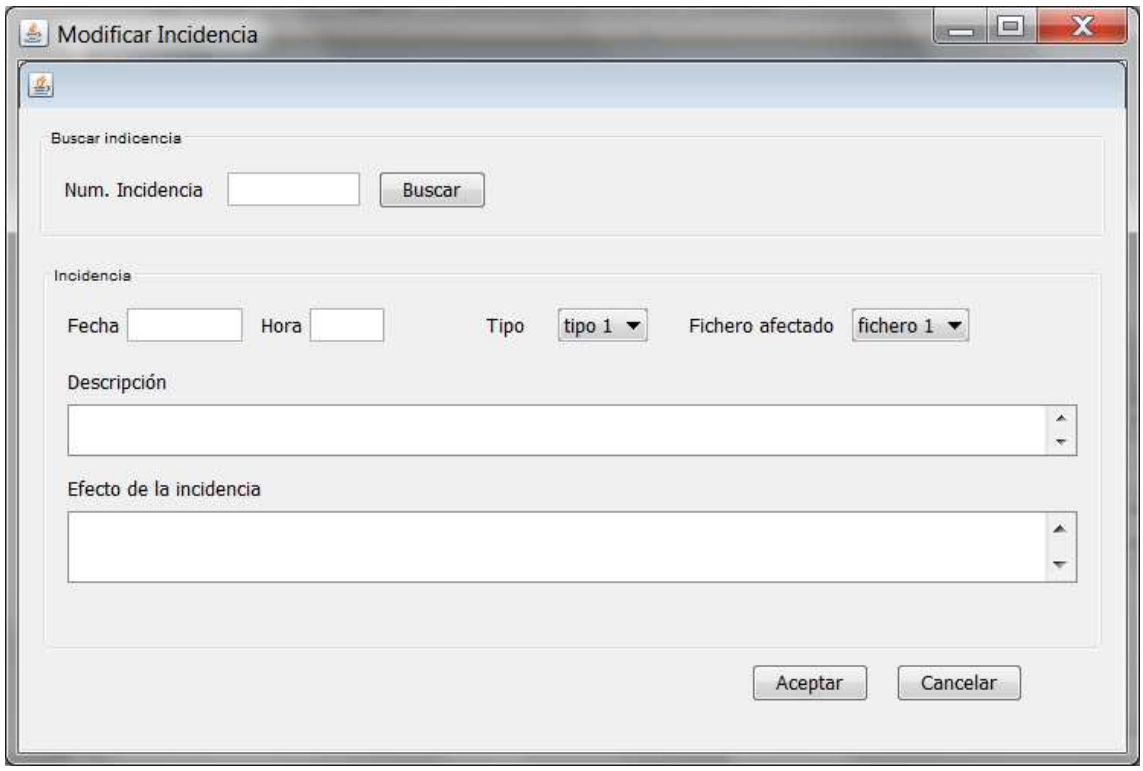
3.3.2. Subsistema de registro de incidencias.



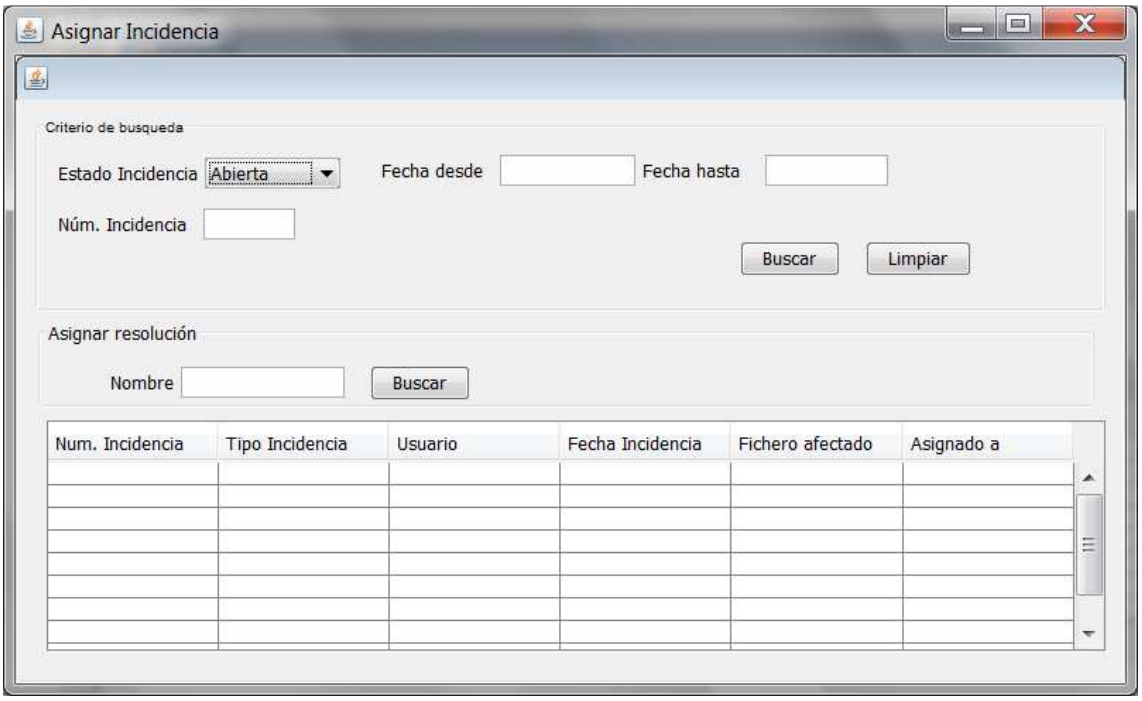
Cualquier usuario del sistema podrá realizar un alta de incidencia

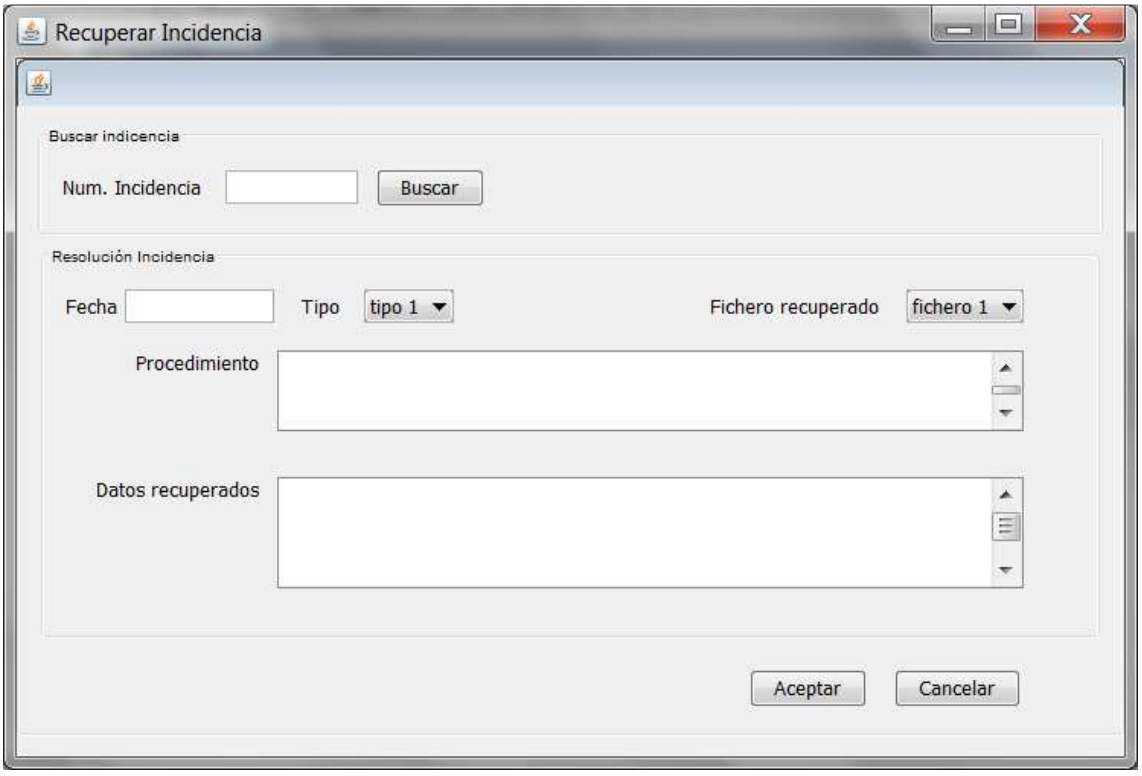


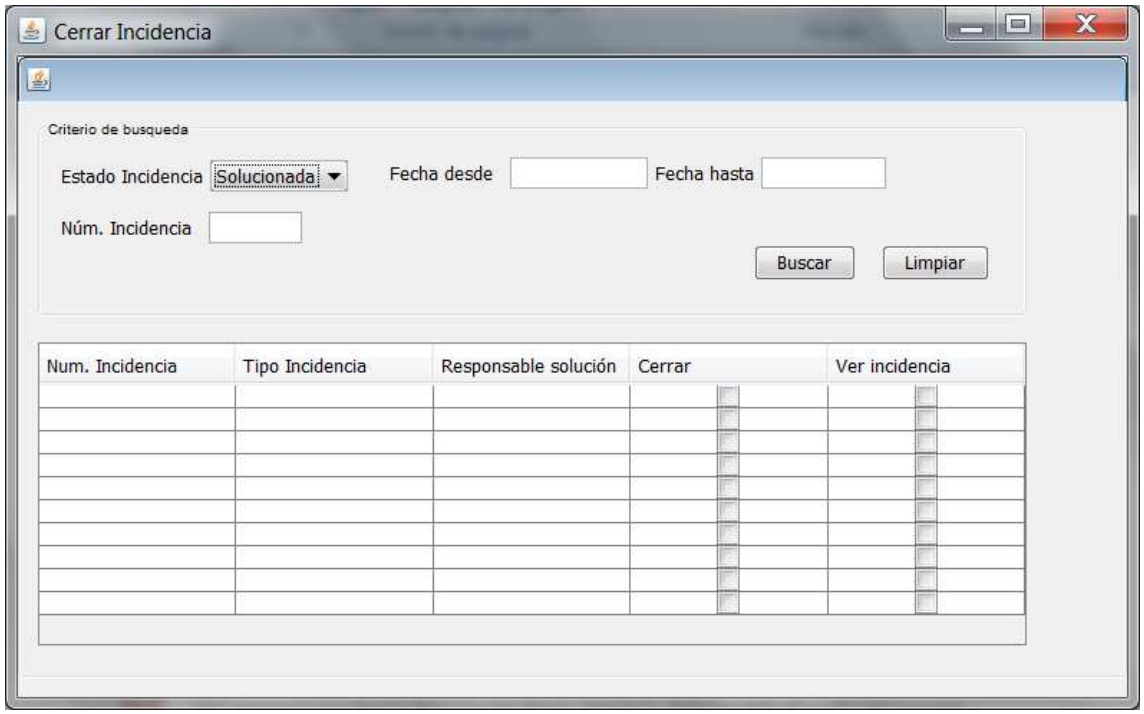
La modificación de las incidencias corresponde al usuario que ha realizado el alta de dicha incidencia.



En la pantalla de asignación de incidencias podremos realizar búsquedas entre fechas, nos mostrará una lista de todas las incidencias dadas de alta en esas fechas. También permite buscar una incidencia concreta, introduciendo el número de incidencia.

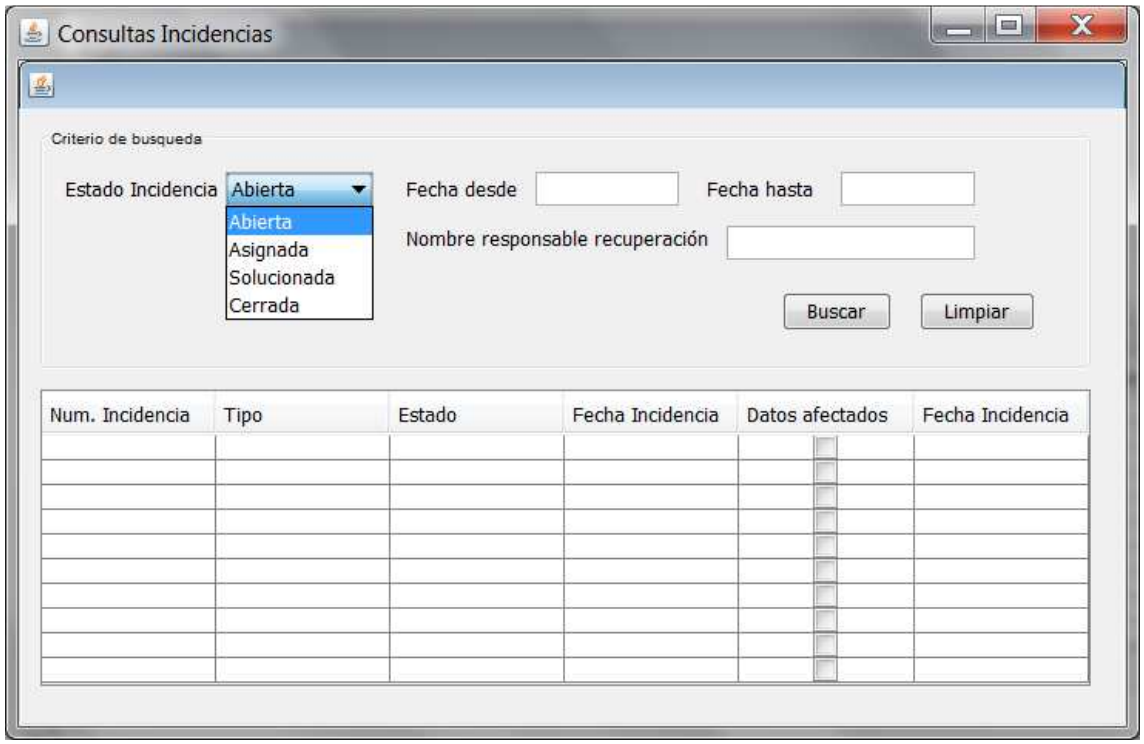


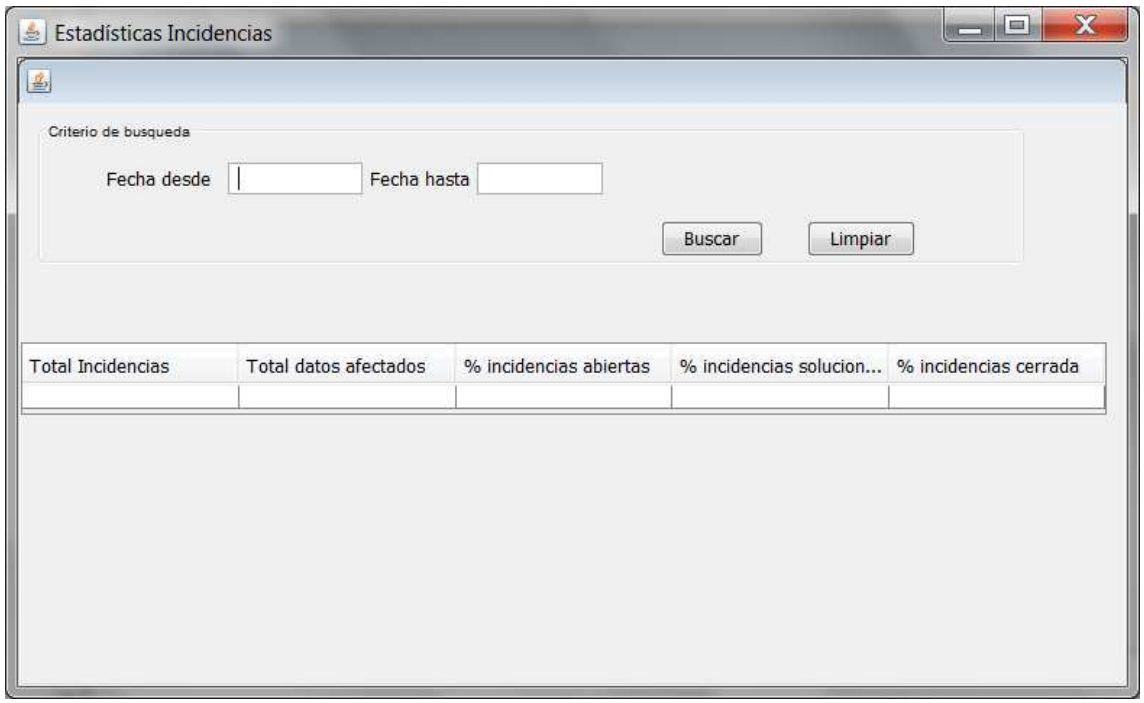



Cerrar Incidencia
Criterio de busqueda
Estado Incidencia
Solucionada
Fecha desde
Fecha hasta
Núm. Incidencia
Buscar
Limpiar
Num. Incidencia
Tipo Incidencia
Responsable solución
Cerrar
Ver incidencia

3.2.3. Subsistema de consulta y estadísticas de incidencias.

Las consultas de incidencias tendrán distintos criterios de búsqueda, por estado, entre dos fechas dadas y por nombre de responsable de recuperación. Sólo es posible establecer un criterio de búsqueda cada vez.





El menú desplegable “Ayuda” dispone de dos opciones uno de información acerca de la aplicación y otro que mostrará una guía de uso de la misma.

Los mensajes informativos y de errores que se produzcan tendrán una única ventana de presentación. Dispone de un campo variable donde se irán mostrando estos mensajes.

Bibliografía, material consulta.

Anexo VI. Registro de incidencias.

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf

REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf

Materiales .

TFC

http://materials.cv.uoc.edu/continguts/XW08_19018_00443/index.html

Ingeniería del Software

http://materials.cv.uoc.edu/cdocent/WEYM7G_2CZ_LIHFIBOEB.pdf

http://materials.cv.uoc.edu/cdocent/TE0F4CX1PH5MCQ4VG9B2.pdf

Técnicas del desarrollo del Software

http://materials.cv.uoc.edu/cdocent/BH8TCXR1JXDJ41G3C0_I.pdf

Anexo.

Software utilizado para la elaboración de este documento:

Edición de texto: *Microsoft Word 2007*

Diagramas de clase, secuencia, estado y excepciones: *MagicDraw 11.0*

Diagramas de casos de uso: *Visual Paradigm*

Diseño de interfaces de usuario: *NetBeans IDE 7.1*

Diagramas de Gantt: *GanttProject*