



# **UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS**

## **FACULTAD 7**

Trabajo de Diploma para Optar por el Título de  
Ingeniero en Ciencias Informáticas

**Componente para el control de acceso y activos fijos en el Sistema de información  
Hospitalaria xavia HIS, utilizando la tecnología de Identificación por Radiofrecuencia**

### **Autores:**

Yisel Navarro Bouzo

Alejandro García Pérez

### **Tutores:**

Ing. Alfredo Rodríguez Ruiz

Ing. Diana Rosa Alfonso Espinosa

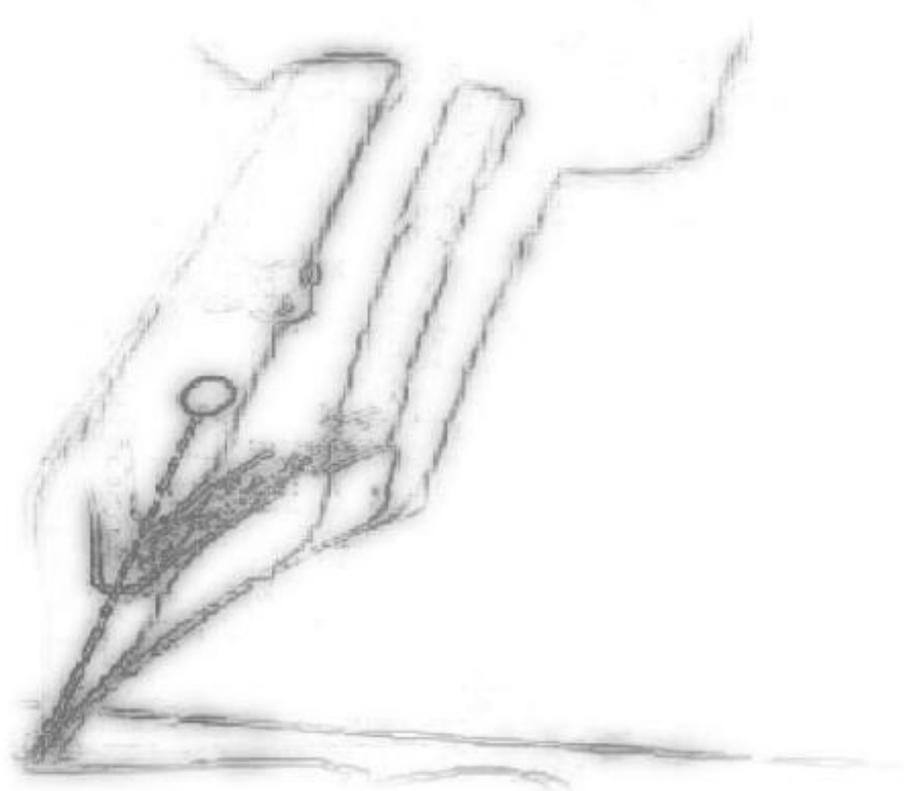
### **Co-Tutor:**

Ing. Reinier Milián Pérez.

**La Habana, Junio de 2013**

**“Año 55 de la Revolución”**

Pensamiento



*“Cuando se es joven, se crea. Cuando se es inteligente, se produce. No se adapta, se innova: la medianía copia; la originalidad se atreve”.*

*José Martí*

### Datos de Contacto

**Ing. Alfredo Rodríguez Ruiz:** Graduado en el año 2008 de Ingeniero en Ciencias Informáticas en la Universidad de las Ciencias Informáticas. Posee categoría docente de Instructor. Ha impartido las asignaturas de Base de Datos, Programación web, Programación 2 y 3 y Gráficos por Computadora. Se desempeña como Jefe del departamento Atención Primaria a la Salud en el Centro de Informática Médica (CESIM). Correo: [arruiz@uci.cu](mailto:arruiz@uci.cu).

**Ing. Diana Rosa Alfonso Espinosa:** Graduada en el año 2008 de Ingeniero en Ciencias Informáticas en la Universidad de las Ciencias Informáticas. Posee categoría docente de Instructor. Ha impartido las asignaturas de Pruebas y Evaluación de Software, Administración de Calidad, CMMI, Aplicaciones informáticas en el sector de la salud e Introducción a las pruebas de software. Se desempeña como analista del departamento Atención Primaria a la Salud en el Centro de Informática Médica (CESIM). Correo: [dralfonso@uci.cu](mailto:dralfonso@uci.cu).

**Ing. Reinier Milián Pérez:** Graduado en el año 2012 de Ingeniero en Ciencias Informáticas en la Universidad de las Ciencias Informáticas. Se desempeña como programador del departamento Atención Primaria a la Salud en el Centro de Informática Médica (CESIM). Correo: [rmilianp@uci.cu](mailto:rmilianp@uci.cu).

## Agradecimientos

De Yisel

La Revolución por darme la posibilidad de estudiar en una Universidad de Excelencia como lo es la Universidad de las Ciencias Informáticas.

Al Comandante Fidel Castro por haber pensado en nosotros como la generación del futuro.

A mis padres, mi tía Odalys, mis hermanos, mi novio Yuniel, mi abuela Orquidea, mi prima Anilexis por todo el esfuerzo que han hecho y el apoyo que me han dado para lograr mi sueño.

A los tutores Diana Rosa y Alfredo que nos han sabido guiar por el camino correcto.

Al tribunal y mi oponente Beatriz por estar al tanto de cada paso en los detalles finales.

A mi compañero Alejandro de tesis por su sacrificio y generosidad, por su ayuda constante y su preocupación.

A mis amigos, compañeros y vecinos de la vida que siempre estuvieron ahí para mí.

A todos aquellos que de una forma u otra me ayudaron en el desarrollo de este trabajo.

Por su dedicación y esmero,

¡Muchas Gracias!

De Alejandro

Quiero agradecer a mis familiares por darme su apoyo incondicional y confianza durante toda la carrera; a mis amigos porque siempre me enseñaron que podía llegar hasta el final, a los profesores que durante cinco años batallaron cada día por hacernos alguien mejor, a mis compañeros del grupo que de una forma u otra aportaron su grano de arena en la elaboración de esta tesis y compartieron junto a mi momentos de alegría y tristezas. A mi compañera de tesis Yisel por su abnegación y sacrificio para salir adelante a cada momento. A todas las personas que me guiaron hasta donde estoy hoy, gracias de todo corazón.

## Dedicatoria

De Yisel

A mis compañeros y amigos que siempre estuvieron a mi lado y dieron su aporte para lograr hacer mi sueño realidad. A mi novio Yuniel por haberme ayudado en todo momento y estar siempre dispuesto brindándome su apoyo incondicional. A mi tía Odalys que ha sido como mi segunda madre, siempre preocupada y dispuesta a dar cualquier paso por mí. A mis hermanos que me han dado todo el apoyo del mundo y su ayuda en lo que han podido. A mi abuela Orquídea por ser, a pesar de sus condiciones físicas la que más me ha impulsado a lograr mis sueños con grandeza. A mi papá por ser uno de los responsables de la persona en que me he convertido hoy. A mi mamá porque a pesar de todas las dificultades siempre ha sabido afrontar con inteligencia y dulzura todos los disturbios ocurridos en estos 5 años de mi carrera, por tener siempre una respuesta convincente, darme fuerzas, sonreírme y lo más importante apoyarme en los momentos en que más la he necesitado.

Yisel Navarro Bouzo

De Alejandro

Dedico este trabajo a toda mi familia y en especial a dos personas que amo mucho y siempre me han enseñado a perseguir mis sueños: mi madre Ileana y mi abuela Lidia. A mi hermano Luisito que se gradúa junto a mí en este trabajo ya que fue el que enseñó a no rendirme jamás y siempre llegar al final. A la nueva alegría de nuestra familia mi sobrinito Frank Alberto por llenarnos el corazón de momentos felices en cada minuto, a mi tía Baby a la cual quiero como una madre, a mis tíos y primos que siempre han estado para compartir cada momento junto de felicidad. A mí cuñada que tanto quiero Maylis, a Gladys por quererme y aceptarme como un hijo más de la familia. A Nereida por sus aportes incondicionales en la realización de esta investigación. A mis amigos Nayibis y Juan Carlos con los cuales siempre pude contar. A Yise por toda su dedicación y excelente trabajo. En general a todas las amistades que me dieron fuerzas para seguir adelante por malos que fueran los tiempos, a todos los que me preguntaron alguna vez como iba la tesis, a todos mil gracias, ya que sin ustedes no podría haberlo conseguido.

Alejandro García Pérez

## Resumen

La tecnología de Identificación por Radiofrecuencia RFID (RadioFrequency Identification) es, sin duda, una de las tecnologías de comunicación que ha experimentado un crecimiento acelerado y sostenido en los últimos tiempos. Las posibilidades que ofrece la lectura de la información contenida en una etiqueta, a distancia, sin necesidad de contacto físico, abre la puerta a un conjunto muy extenso de aplicaciones en diferentes ámbitos, desde la trazabilidad y control de activos, hasta la localización y seguimiento de personas, o la seguridad en el control de acceso.

A partir de un estudio realizado se demostró la necesidad de integrar esta tecnología al sistema xavia HIS desarrollado en el Centro de Informática Médica (CESIM), ya que proporciona un incremento de la seguridad, así como un mayor control de los activos, reduciendo los costes por pérdidas en las entidades sanitarias y un mejor control de las áreas restringidas.

El desarrollo del componente se encuentra guiado por el proceso de mejora de CMMI, se basa en tecnologías libres, multiplataforma, sobre una arquitectura en capas, utilizando Java como lenguaje de programación. Se emplea el patrón arquitectónico Modelo-Vista-Controlador que facilita la creación de una aplicación robusta y flexible. Como Sistema de Gestión de Bases de Datos es usado el PostgreSQL y como servidor de aplicaciones el JBoss Application Server.

Como resultado se espera disponer de una herramienta que integre los procesos de control de acceso y activos fijos en tiempo real en un solo componente haciendo uso de la Identificación por Radiofrecuencia.

**Palabras Clave:** activos fijos, control de accesos, Identificación por Radiofrecuencia, sistema.

## Tabla de Contenidos

<b>INTRODUCCIÓN.....</b>	<b>1</b>
<b>CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA – METODOLÓGICA DEL CONTROL DE ACCESO Y ACTIVOS FIJOS EN SISTEMAS HOSPITALARIOS .....</b>	<b>6</b>
1.1 RESEÑA HISTÓRICA DE LOS SISTEMAS DE CONTROL DE ACCESO .....	6
1.2 SISTEMA DE CONTROL DE ACCESO .....	6
1.3 IDENTIFICACIÓN POR RADIOFRECUENCIA .....	10
1.4 COMPONENTES DE LA IDENTIFICACIÓN POR RADIOFRECUENCIA.....	11
1.5 PROTOCOLOS DE COMUNICACIÓN.....	15
1.6 SISTEMAS DE IDENTIFICACIÓN POR RADIOFRECUENCIA INTEGRADOS A LOS PROCESOS DE CONTROL DE ACCESO Y ACTIVOS FIJOS .....	15
1.7 PATRONES Y LENGUAJES UTILIZADOS.....	17
1.8 GUÍA DE DESARROLLO DE SOFTWARE .....	21
1.9 HERRAMIENTAS Y TECNOLOGÍAS UTILIZADAS PARA LA SOLUCIÓN .....	22
<b>CAPÍTULO 2. DISEÑO DEL SISTEMA PARA EL CONTROL DE ACCESO Y ACTIVOS FIJOS.....</b>	<b>26</b>
2.1 ACTORES DEL NEGOCIO .....	26
2.2 DESCRIPCIÓN DE LOS PROCESOS DEL NEGOCIO .....	27
2.3 PROPUESTA DEL SISTEMA .....	30
2.4 ESPECIFICACIÓN DE LOS REQUISITOS DE SOFTWARE.....	31
2.5 MODELO DEL ANÁLISIS .....	37
2.6 MODELO DEL DISEÑO .....	40
2.7 DIAGRAMAS DE CLASES DEL DISEÑO.....	44
2.8 MODELO DE DATOS. ....	47
2.9 SELECCIÓN DE EQUIPOS Y ANÁLISIS DE COSTO.....	49
<b>CAPÍTULO 3: IMPLEMENTACIÓN DEL SISTEMA PARA EL CONTROL DE ACCESO Y ACTIVOS FIJOS.....</b>	<b>52</b>
3.1 INTEGRACIÓN CON OTROS SISTEMAS.....	52
3.2 DIAGRAMA DE DESPLIEGUE .....	52
3.3 DIAGRAMA DE COMPONENTES .....	54
3.4 TRATAMIENTO DE EXCEPCIONES.....	55
3.5 SEGURIDAD.....	57
3.6 PRINCIPALES FUNCIONALIDADES .....	57
3.7 ESTÁNDAR DE CODIFICACIÓN .....	60
<b>CONCLUSIONES.....</b>	<b>62</b>
<b>RECOMENDACIONES.....</b>	<b>63</b>
<b>REFERENCIAS BIBLIOGRÁFICAS .....</b>	<b>634</b>
<b>BIBLIOGRAFÍA.....</b>	<b>67</b>
<b>GLOSARIO DE TÉRMINOS .....</b>	<b>70</b>
<b>ANEXOS .....</b>	<b>72</b>

## Índice de Figuras

FIGURA 1.1. TARJETA CON CINTA MAGNÉTICA.....	7
FIGURA 1.2. CÓDIGO DE BARRAS.....	8
FIGURA 1.3. TARJETAS INTELIGENTES.....	8
FIGURA 1.4 CLAVE POR TECLADO.....	9
FIGURA 1.5 SISTEMA BIOMÉTRICO.....	9
FIGURA 1.6. SISTEMA DE IDENTIFICACIÓN POR RADIOFRECUENCIA.....	10
FIGURA 1.7. ETIQUETAS PASIVAS.....	12
FIGURA 1.8. ETIQUETAS ACTIVAS.....	12
FIGURA 1.9. ETIQUETAS SEMIPASIVAS.....	13
FIGURA 1.10. LECTORES FIJOS RFID.....	13
FIGURA 1.11. LECTORES PORTÁTILES RFID.....	14
FIGURA 1.12. SIMULADOR RIFIDI PROTOTYPER.....	24
FIGURA 2.1. DCA CREACIÓN DE ÁREAS EN LA ENTIDAD.....	27
FIGURA 2.2. DCA INGRESO DE ACTIVOS FIJOS TANGIBLES.....	28
FIGURA 2.3. DCA TIPOS DE MEDIOS.....	29
FIGURA 2.4. DCA TIPO DE ACCESO AL PERSONAL.....	30
FIGURA 2.5. DCA ADICIONAR AFT.....	38
FIGURA 2.6. DCA ADICIONAR PERSONAL EXTERNO A LA ENTIDAD.....	39
FIGURA 2.7. DCA MONITORIZAR AFT POR ÁREA.....	39
FIGURA 2.8. DCA MONITORIZAR ACCESO POR ÁREA.....	40
FIGURA 2.9. PATRÓN ARQUITECTÓNICO MODELO VISTA CONTROLADOR.....	40
FIGURA 2.10. PATRÓN DE DISEÑO EXPERTO.....	42
FIGURA 2.11. PATRÓN DE DISEÑO CREADOR.....	42
FIGURA 2.12. PATRÓN DE DISEÑO BAJO ACOPLAMIENTO.....	43
FIGURA 2.13. DCD ADICIONAR AFT.....	44
FIGURA 2.14. DCD ADICIONAR PERSONAL EXTERNO A LA ENTIDAD.....	45
FIGURA 2.15. DCD MONITORIZAR AFT POR ÁREA.....	45
FIGURA 2.16. DCD MONITORIZAR ACCESO POR ÁREA.....	46
FIGURA 2.17. MODELO DE DATOS.....	48
FIGURA 3.1. DIAGRAMA DE DESPLIEGUE.....	53
FIGURA 3.2. DIAGRAMA DE COMPONENTES.....	55
FIGURA 3.3. TRATAMIENTO DE EXCEPCIONES.....	56
FIGURA 3.4. MONITORIZACIÓN DEL PERSONAL POR ÁREAS.....	58
FIGURA 3.5. MONITORIZACIÓN DE ACTIVOS FIJOS POR ÁREAS.....	59
FIGURA 3.6. SISTEMA DE ACTIVACIÓN DE ALARMAS POR ÁREAS.....	59
FIGURA 3.7. NOTIFICACIONES DE ANOMALÍAS REGISTRADAS.....	60

## Índice de Tablas

TABLA 2.1. ACTORES DEL NEGOCIO .....	26
TABLA 2.2. DESCRIPCIÓN DE LAS CLASES DEL ANÁLISIS .....	37
TABLA 2.3. DESCRIPCIÓN DE LAS CLASES DEL DISEÑO .....	46
TABLA 2.4. ETIQUETA UHF .....	49
TABLA 2.5. LECTOR GEN2 DE LARGO ALCANCE .....	49
TABLA 2.6. LECTOR USB RFID UHF DE ESCRITORIO .....	50
TABLA 2.7. ANTENA ALIEN CIRCULAR.....	50
TABLA 2.8. PRECIOS DE EQUIPOS RFID .....	50

## Introducción

En los últimos años ha ocurrido un cambio de paradigma debido al modo en que el hombre ve y hace las cosas. El desarrollo tecnológico muestra una convergencia entre la Informática, las Telecomunicaciones, la Electrónica y la Automatización, proceso que ha devenido una nueva rama del saber denominada Tecnologías de la Información y las Comunicaciones (TIC). Ostentando una alta incidencia en la modernización y eficiencia de todos los sectores de la sociedad, constituyendo una herramienta útil para enfrentar el reto que representa vivir en una sociedad que se desarrolla progresivamente (1).

Muchos han sido los sectores beneficiados en este ámbito: el sector de la salud es uno de los favorecidos ampliamente con el empleo de las TIC, en el logro del cumplimiento de sus funciones esenciales. La complejidad de las especialidades médicas, la necesidad de mejorar las prestaciones al paciente y los problemas en el manejo del gran cúmulo de información, fueron los detonadores principales para utilizar la informática en todos los sectores de los servicios sanitarios.

Entre las tecnologías emergentes con gran impacto en la sociedad se pueden mencionar los códigos de barras, cintas magnéticas, tarjetas inteligentes (2), sistemas biométricos (3) y la Identificación por Radiofrecuencia (RFID, por sus siglas en inglés) (4). Sus principales potencialidades están enmarcadas en muchos de los sectores industriales.

La Identificación por Radiofrecuencia es apoyada por grandes compañías y básicamente captura e identifica de forma automática la información contenida en etiquetas (tags o transpondedores) que son adheridas a cualquier objeto o persona (5). Cuando las etiquetas entran en el área de cobertura de un lector RFID, éste envía una señal para que la misma transmita la información almacenada en su memoria.

Como resultado de los avances tecnológicos que se han llevado a cabo en el sector de la Salud y dentro de las soluciones informáticas se destacan los Sistemas de Información Hospitalaria (HIS, por sus siglas en inglés) (6). Los HIS tienen como objetivo la gestión de la información en instituciones hospitalarias. Constituyen un apoyo para las actividades en los niveles operativos, estratégicos y tácticos de cualquier institución hospitalaria, pues están orientados a satisfacer las necesidades de almacenamiento, procesamiento, recopilación, recuperación e interpretación de los datos médico-administrativos generados.

En las instituciones hospitalarias el proceso de control de acceso al personal se lleva a cabo mediante el control del personal interno y externo a las diversas áreas de la entidad hospitalaria. El control interno se realiza cuando el personal que labora en la unidad tales como médicos, enfermeras, directivos de la institución, entre otros, se identifican mostrando su credencial a los agentes de seguridad. Los agentes verifican la validez de la credencial mostrada.

Por su parte el control externo es realizado cuando personas que no laboran directamente en la unidad de salud arriban a la misma. Este tipo de personal puede categorizarse en visitas, pacientes u otros directivos ajenos a la entidad. A todos ellos se les otorga una identificación de carácter temporal que les permite acceder a las áreas de la institución.

Los activos fijos son los bienes destinados a la institución por algún proveedor y se controlan por el responsable del almacén. Cuando llegan activos a la entidad el contador general recibe la factura y la envía al departamento de contabilidad de la unidad. Luego de que el departamento de contabilidad y el responsable del almacén concilian el cargamento recibido, es enviado un informe al contador general, el cual se encarga de archivarlo.

Como un tipo de HIS desarrollado por el Centro de Informática Médica (CESIM) perteneciente a la Universidad de las Ciencias Informáticas (UCI), se menciona el sistema xavia HIS. El mismo está compuesto por varios módulos que gestionan la información manipulada por las distintas áreas de una institución hospitalaria.

A pesar del desarrollo que ha alcanzado el sistema xavia HIS aún presenta las siguientes debilidades:

- Carece de un mecanismo que realice el control de acceso y la monitorización en tiempo real del personal que accede a la institución, limitando la posibilidad de identificar cualquier violación de acceso en el momento en que ocurra.
- Retrasa la generación de reportes estadísticos relacionados a la identificación de las personas que han visitado un área determinada dentro de la institución médica, lo que dificulta el control de acceso a las zonas restringidas de dicha entidad.
- No posee un sistema de alarmas que informe si un activo fijo ha sido retirado de su área con previa autorización, por lo que difiere con la posibilidad de identificar a tiempo el desvío o pérdida de los recursos materiales de la institución.

Dada la situación planteada anteriormente el **problema a resolver** consiste en: ¿Cómo integrar la tecnología de Identificación por Radiofrecuencia a los procesos de control de acceso y activos fijos en tiempo real en el Sistema de Información Hospitalaria xavia HIS, que contribuya a la monitorización del personal y los activos fijos?

Para dar respuesta al problema anterior se toma como **objeto de estudio**: los procesos de control de acceso y activos fijos en tiempo real en los Sistemas de Información Hospitalaria, enmarcando el **campo de acción** en la gestión del control de acceso y activos fijos en tiempo real para el Sistema de Información Hospitalaria xavia HIS.

Se concibió como **objetivo general**: desarrollar un componente informático que utilice la tecnología de Identificación por Radiofrecuencia para los procesos de control de acceso y activos fijos en tiempo real en el Sistema de Información Hospitalaria xavia HIS que contribuya a la monitorización del personal y los activos fijos.

Por tal razón se plantea la siguiente **idea a defender**: si se desarrolla un componente informático que utilice la tecnología de Identificación por Radiofrecuencia para los procesos de control de acceso y activos fijos en tiempo real del Sistema de Información Hospitalaria xavia HIS contribuirá a la monitorización del personal y los activos fijos.

Para lograr el objetivo propuesto se dará cumplimiento a las siguientes **tareas de investigación**:

- I. Caracterización de la génesis y evolución de la tecnología RFID.
- II. Establecimiento de las características y capacidades de los diferentes sistemas que utilizan la tecnología RFID para el control de acceso y activos fijos en áreas determinadas de una institución de salud.
- III. Establecimiento de los procesos de control de acceso y activo fijos haciendo uso de la tecnología RFID en el sistema xavia HIS.
- IV. Desarrollo del componente informático aplicando las pautas de diseño definidas por el CESIM, siguiendo lo establecido en la Especificación de Requisitos de Software.
- V. Integración del componente informático para el sistema xavia HIS.

Para la realización de esta investigación se siguió una estrategia descriptiva, donde se refleja lo más esencial y significativo, utilizándose los siguientes métodos investigativos:

### **Métodos Teóricos:**

- **Histórico-Lógico:** se utiliza para realizar un estudio sobre las aplicaciones informáticas que utilicen la tecnología RFID implementadas en Cuba y en el mundo.
- **Analítico-Sintético:** se hace uso del mismo para resumir, enunciar y describir los requerimientos funcionales que debe detallar el sistema que se propone.
- **Modelación:** para realizar una reproducción simplificada de la realidad y generar los artefactos correspondientes a los flujos de trabajo en los que se trabajará para estudiar y transformar el objeto de estudio.

### **Métodos Empíricos:**

Como uno de los métodos empíricos utilizados se empleó la entrevista, específicamente la no estructurada o libre.

- **Entrevista no estructurada o libre:** se realizan preguntas abiertas a los líderes del sistema xavia HIS, sin tener un orden preestablecido de las mismas adquiriendo las características de la conversación y realizando las preguntas en correspondencia a las respuestas que surgían para comprender la situación real del problema existente, así como las opiniones y propuestas de los mismos.
- **Observación:** para realizar un registro visual de lo que ocurre en el sistema xavia HIS y aportar nuevos elementos que mejoren su funcionamiento.
- **Experimento:** para validar la transformación de los procesos de control de acceso y activos fijos en el sistema xavia HIS, aplicando mediante el simulador la solución planteada.

El presente documento está estructurado en tres capítulos, que incluyen todo lo relacionado con el trabajo investigativo, así como el diseño e implementación del sistema.

**CAPÍTULO 1. Fundamentación teórica – metodológica del control de acceso y activos fijos en sistemas hospitalarios:** se describen los conceptos generales de la investigación así como los sistemas informáticos existentes en el ámbito nacional e internacional. Se describen además las características de las herramientas, metodologías y tecnologías propuestas para la realización del componente.

**CAPÍTULO 2. Diseño del componente para el control de acceso y activos fijos:** se describen los procesos involucrados y se analizan las actividades que serán objeto de automatización, además los requerimientos con que debe contar el sistema, así como los patrones del diseño utilizados. Conjuntamente se representa la concepción arquitectónica del sistema con el objetivo de entender la estructura y dinámica de la organización del mismo.

**CAPÍTULO 3. Implementación del componente para el control de acceso y activos fijos:** describe los componentes informáticos fundamentales de todo el proceso de implementación, así como los métodos, estándares de diseño, codificación y excepciones, y por último la representación general del diagrama de despliegue con los artefactos generados en esta fase.

Se concluye el documento con un conjunto de acciones futuras para la implementación de la estrategia propuesta y las correspondientes recomendaciones. Se hace referencia a los beneficios que se esperan con el desarrollo del componente presentado, además se muestra un gran cúmulo de referencias bibliográficas de las fuentes utilizadas a lo largo del contenido y la bibliografía consultada para un mejor entendimiento de la investigación, así como un resumen de los términos que puedan causar dificultad al intelecto del cliente.

## **Capítulo 1. Fundamentación teórica – metodológica del control de acceso y activos fijos en sistemas hospitalarios**

El objetivo fundamental de este capítulo es abordar los aspectos que se utilizan como soporte teórico del componente a diseñar e implementar. Se exponen a través de una descripción de los conceptos asociados al problema, así como el estudio del estado del arte referente al control de acceso y activos fijos en la gestión hospitalaria en tiempo real, haciendo uso de la tecnología RFID a nivel nacional e internacional. Además se presentan las características de las herramientas, metodologías y tecnologías escogidas para la solución del problema, se argumenta la elección de las mismas y la utilidad de las tecnologías de la informática y las comunicaciones.

### **1.1 Reseña histórica de los sistemas de control de acceso**

Control de acceso es la habilidad de permitir o denegar el uso de un recurso por una persona o entidad en particular. Los mecanismos de acceso de control pueden ser usados en el manejo de recursos físicos, recursos lógicos o recursos digitales. Con referencia estrictamente al manejo de recursos físicos, el término control de acceso se refiere a la práctica de restringir la entrada a un bien inmueble, edificio, cuarto o a un área específica, únicamente a personas autorizadas. Un control de acceso físico puede ser logrado por seres humanos (guardia, portero o recepcionista), o por medios mecánicos como cerraduras y llaves, los cuales han sido utilizados por más de 4000 años.

El control de acceso físico se engloba en tres hechos fundamentales: quién, cómo y cuándo. Un sistema de control determina quien está permitido a entrar o salir, donde está permitido a entrar o salir y cuando está permitido a entrar o salir. Históricamente esto era muy parcialmente conseguido a través de cerraduras y llaves.

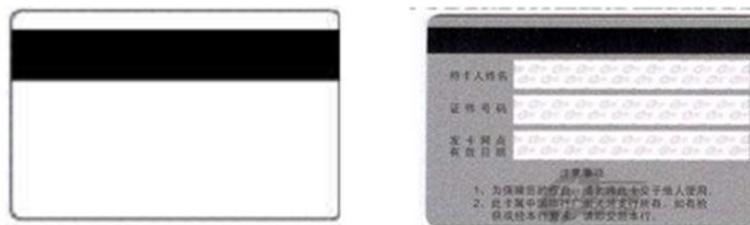
### **1.2 Sistema de control de acceso**

El avance de la tecnología permite que el control de acceso electrónico resuelva las limitaciones de las cerraduras mecánicas y llaves, utilizando nueva tecnologías se puede realizar el control de las cerraduras y almacenar la información necesaria acerca de tiempos, fechas de ingreso de personas autorizadas, tentativas de ingreso de personas no autorizadas, así como monitorizar alarmas, en caso de que la puerta sea forzada (7). En esta sección se describen las principales tecnologías usadas actualmente en los sistemas de control de acceso.

## 1.2.1 Cintas magnéticas

Es la tecnología más conocida y difundida, dado que se utiliza en todos los sistemas de tarjeta de crédito y de compra. El lector identifica al usuario leyendo el código inscrito en la cinta magnética que está adherida a la tarjeta. Sus ventajas son su difusión, popularidad y bajo costo; sin embargo, la banda magnética de la tarjeta, debe ser tratada con cierto cuidado debido a que puede rayarse o si es expuesta a campos magnéticos su código puede borrarse. Por tal motivo no son recomendables por ejemplo para usar en ambientes industriales (8).

La figura 1.1 muestra dos tipos de tarjeta con cinta magnética.



**Figura 1.1. Tarjeta con cinta magnética**

**Fuente:** <http://www.cavsi.com/preguntasrespuestas/que-es-una-cinta-magnetica/&dt=-&s=-&r=DQE>

## 1.2.2 Códigos de barra

El código de barras es un código basado en la representación mediante un conjunto de líneas paralelas verticales de distinto grosor y espaciado que en su conjunto contienen una determinada información. La ventaja de usar la tecnología de código de barras es que es barata, y es muy sencillo generar la identificación que puede ser fácilmente aplicada a tarjetas u otros elementos. Su desventaja es que es muy vulnerable a falsificaciones y el lector puede tener problemas con identificaciones sucias, borrosas o manchadas. Es por esto que actualmente existen otras tecnologías más seguras, y el código de barras se ha dejado de utilizar, a pesar de que fue la primera en ser usada para realizar control de acceso (9).

La figura 1.2 muestra una imagen del código de barras.



**Figura 1.2. Código de barras**

**Fuente:** <http://www.barcodeart.com/science/science.html>

### **1.2.3 Tarjetas inteligentes**

Una tarjeta inteligente (*Smart Card*), o tarjeta con circuito integrado, es una tarjeta plástica que contiene un pequeño microprocesador que es capaz de hacer diferentes cálculos, guardar información y manejar programas, que están protegidos a través de mecanismos avanzados de seguridad. Existen dos categorías principales: las tarjetas de memoria que contienen solo componentes no volátiles y las tarjetas microprocesadoras las cuales contienen memoria y microprocesadores (10).

A continuación la figura 1.3 muestra tarjetas inteligentes.



**Figura 1.3. Tarjetas inteligentes**

**Fuente:** <http://spanish.am-labels.com>

### **1.2.4 Clave por teclado**

Consiste en un número personal de identificación, el cual puede variar de cuatro a ocho dígitos. La ventaja de usar un número de identificación es que una vez que se ha memorizado el número, esta “credencial” no puede ser perdida u olvidada en algún lugar. La desventaja es la dificultad que algunas personas tienen en recordar números, y que la clave puede ser observada y consecuentemente usada por personas no autorizadas. Obviamente esta opción es la más económica, pero la menos segura. Hace tiempo que han caído en desuso y no se han generado hasta el momento nuevas aplicaciones donde puedan resurgir como una opción válida (11).

# CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA- METODOLOGICA DEL CONTROL DE ACCESO Y ACTIVOS FIJOS EN SISTEMAS HOSPITALARIOS

---

A continuación la figura 1.4 muestra una imagen de la clave por teclado.



**Figura 1.4 Clave por teclado**

**Fuente:** [www.olimpiahardware.com/access-control/index.html](http://www.olimpiahardware.com/access-control/index.html)

## 1.2.5 Sistema biométrico

Su funcionamiento se basa en la lectura de alguna parte del cuerpo humano, eliminando por completo el uso de las tarjetas. Los más conocidos pueden ser los lectores de huellas digitales, geometría de la mano e iris del ojo. Su principal ventaja radica en la seguridad, ya que por su esencia es intransferible. Sus principales desventajas radican en el precio del lector, la velocidad de lectura y por último la poca posibilidad de ser autónomos (12).

A continuación la figura 1.5 muestra una imagen de los sistemas biométricos.



**Figura 1.5 Sistema biométrico**

**Fuente:** [www.accesor.com/esp/lectores\\_biometria.php](http://www.accesor.com/esp/lectores_biometria.php)

Una vez que se han analizados las diferentes tecnologías así como los conceptos generales utilizados en los sistemas de control de acceso, se estudiará a continuación la tecnología de identificación por radiofrecuencia.

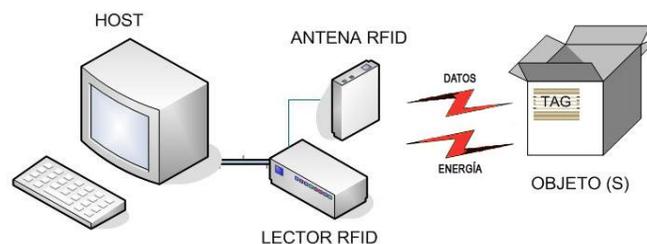
## 1.3 Identificación por Radiofrecuencia

La tecnología RFID ha ido despertando las expectativas de un número cada vez mayor de sectores industriales, interesados por sus funcionalidades. Los primeros en utilizar RFID aseguran que conducirá a eficiencias sin precedentes en todos los campos que se utilice. En términos generales, RFID es una tecnología de identificación a personas u objetos en forma remota e inalámbrica. Del mismo modo esta tecnología puede ser usada para identificar, rastrear, ordenar o detectar una amplia variedad de objetos (13).

Son muchas las grandes compañías que apoyan la implantación y el uso sensato de la RFID, por lo que se puede esperar que su futuro sea muy prometedor. No hay duda de que se trata de una tecnología que puede aportar sustanciales ventajas en muchos ámbitos de aplicación. Sin embargo, el éxito final en la implantación de esta tecnología está sujeto a la superación de una serie de obstáculos, entre los que es necesario destacar los aspectos de seguridad y privacidad.

El funcionamiento de los sistemas RFID es simple, y son necesarios dos elementos básicos: una etiqueta electrónica y un lector. Básicamente lo que ocurre es que cuando se enciende el lector, este empieza a emitir una señal a una frecuencia previamente establecida. Cualquier etiqueta que esté asociada a ese lector y que se encuentre en su proximidad, detectará la señal y usando la energía de la misma, hará funcionar sus circuitos internos. Una vez que la etiqueta haya decodificado la señal como válida, enviará una respuesta al lector enviando la información que contiene en forma de señales de radio modulada (14).

A continuación la figura 1.6 muestra una imagen de la tecnología RFID con sus componentes específicos.



**Figura 1.6. Sistema de identificación por radiofrecuencia**  
**Fuente: Blazquez del Toro, L. Sistemas de Identificación por Radiofrecuencia**

## 1.4 Componentes de la identificación por radiofrecuencia

Existe una gran diversidad de sistemas RFID, los cuales pueden satisfacer un amplio abanico de aplicaciones para los que pueden ser utilizados. Sin embargo, a pesar de que los aspectos tecnológicos pueden variar, todos se basan en el mismo principio de funcionamiento el cual se compone de 4 elementos fundamentales: etiqueta, lector, ordenador y middleware.

### 1.4.1 Etiquetas

La etiqueta es el elemento que detecta la señal del lector y envía la información que contiene, la cual puede ir desde un código único hasta información más detallada del objeto al cual está adherido. Las etiquetas tienen varias formas, entre las que se incluyen: tarjetas flexibles, llaveros, relojes, piezas metálicas similares a monedas, cintas, papel, e incluso pueden estar dentro de teléfonos celulares. Consta de un microchip que almacena los datos y una pequeña antena que habilita la comunicación por radiofrecuencia con el lector.

La mayoría de las etiquetas RFID internamente poseen una memoria no volátil como memoria ROM Programable y Borrable Eléctricamente (EEPROM, por sus siglas en inglés) para guardar la información. La capacidad de la memoria depende del modelo y va en un rango aproximado de 96 bits para aplicaciones en donde solo se almacena un código, a etiquetas con más de 32 Kbits para almacenar información más detallada, sin embargo esto aumenta el precio de la etiqueta.

Las etiquetas RFID se clasifican dependiendo de la frecuencia de operación y de la programación que se desee emplear:

- **Etiquetas pasivas:** las etiquetas pasivas son aquellas que no poseen ningún tipo de alimentación. La señal que les llega de los lectores induce una corriente eléctrica mínima que basta para operar el circuito integrado de la etiqueta para generar y transmitir una respuesta. Generalmente trabajan a frecuencias bajas, entre 100KHz y 500KHz. En la práctica las etiquetas pasivas suelen tener distancias comprendidas entre los 10 cm y hasta unos pocos metros dependiendo de la frecuencia de funcionamiento, el diseño y principalmente el tamaño de la antena. Su tiempo de vida gira entorno a los 30 años.

A continuación la figura 1.7 muestra una imagen de etiquetas pasivas.



**Figura 1.7. Etiquetas pasivas**

**Fuente: Blazquez del Toro, L. Sistemas de Identificación por Radiofrecuencia**

- **Etiquetas activas:** a diferencia de las etiquetas pasivas, las activas poseen su propia fuente autónoma de energía, que utilizan para dar corriente a sus circuitos integrados y propagar su señal al lector. Estas etiquetas son mucho más fiables (tienen menos errores) que las pasivas, debido a su capacidad de establecer sesiones con el lector. Trabajan a frecuencias altas comprendidas entre los 310MHz y 5.9GHZ y por ende a mayores distancias entre ellas y el lector, con una velocidad de lectura de hasta 2Mbps. También presentan desventajas como son el costo y las dimensiones. Su tiempo de vida gira alrededor de los 10 años.

A continuación la figura 1.8 muestra una imagen de etiquetas activas.



**Figura 1.8. Etiquetas activas**

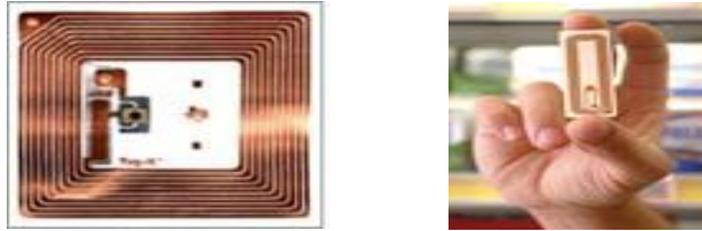
**Fuente: Blazquez del Toro, L. Sistemas de Identificación por Radiofrecuencia**

- **Etiquetas semipasivas:** las etiquetas semipasivas se parecen a las activas en que poseen una fuente de alimentación propia, aunque en este caso se utiliza principalmente para alimentar el microchip y no para transmitir una señal. Este tipo de etiquetas utilizan, al igual que las pasivas, la energía contenida en la radiofrecuencia para transmitir la señal. La batería puede permitir al circuito integrado de la etiqueta estar constantemente alimentado y eliminar la necesidad de diseñar una antena para recoger potencia de una señal entrante. Las etiquetas RFID semipasivas responden más rápidamente y tienen mayores rangos de funcionamiento que las pasivas.

# CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA- METODOLOGICA DEL CONTROL DE ACCESO Y ACTIVOS FIJOS EN SISTEMAS HOSPITALARIOS

---

A continuación la figura 1.9 muestra una imagen de etiquetas semipasivas.



**Figura 1.9. Etiquetas semipasivas**

**Fuente: Blazquez del Toro, L. Sistemas de Identificación por Radiofrecuencia**

## 1.4.2 Lectores

El lector o interrogador es un elemento clave en cualquier sistema RFID, el lector crea el campo y si detecta etiquetas en sus inmediaciones, extrae la información y se la pasa al sistema de procesamiento de datos. Al igual que las etiquetas, contiene una antena, un decodificador y un transceptor; es decir, realiza funciones de transmisión como de recepción y la configuración de los circuitos internos. Este equipo requiere de su propia fuente de alimentación, la antena es capaz de activar en menos de 100mseg varias tarjetas ubicadas dentro de su zona de emisión (15).

A continuación la figura 1.10 muestra una imagen de disímiles lectores fijos utilizados para la tecnología de identificación por radiofrecuencia.



**Figura 1.10. Lectores fijos RFID**

**Fuente: <http://www.dipolerfid.es/Productos/Lectores-RFID/Default.aspx>.**

Los lectores pueden ser clasificados en fijos (*Fixed Reader*) y portátiles (*Mobile Reader*). El primer caso es colocado principalmente en paredes, puertas o cintas transportadoras, por lo cual la antena debe tener

## CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA- METODOLOGICA DEL CONTROL DE ACCESO Y ACTIVOS FIJOS EN SISTEMAS HOSPITALARIOS

---

una polarización lineal; pero el mayor uso es para el segundo en equipos móviles como elevadores, lo que hace que la antena requiera una polarización circular.

A continuación la figura 1.11 muestra una imagen de disímiles lectores portátiles utilizados para la tecnología de identificación por radiofrecuencia.



**Figura 1.11. Lectores portátiles RFID**

**Fuente:** <http://www.dipolerfid.es/Productos/Lectores-RFID/Default.aspx>.

### 1.4.3 Capa intermedia

La capa intermedia (*middleware*, por sus siglas en inglés) es el software que se ocupa de la conexión entre el hardware de RFID y los sistemas de información existentes en la aplicación. Es el encargado de la monitorización, procesamiento, filtraje, modificación y enrutamiento de toda la información captada por los lectores. Los sistemas RFID hardware serían inútiles sin un software que los permita funcionar. Esto es precisamente el *middleware*, por tanto es el máximo responsable de la calidad y usabilidad de las aplicaciones basadas en RFID (16).

Las cuatro funciones principales del *middleware* son:

- Adquisición de datos: el *middleware* es responsable de la extracción, agrupación y filtrado de los datos procedentes de múltiples lectores RFID en un sistema complejo.
- Encaminamiento de los datos: el *middleware* facilita la integración de las redes de elementos y sistemas RFID de la aplicación. Para ello dirige los datos al sistema apropiado dentro de la aplicación.
- Gestión de procesos: el *middleware* se puede utilizar para disparar eventos en función de las reglas de la organización empresarial donde opera.
- Gestión de dispositivos: el *middleware* se ocupa también de monitorizar y coordinar los lectores RFID, así como de verificar su estado y operatividad, y posibilita su gestión remota (17).

# CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA- METODOLOGICA DEL CONTROL DE ACCESO Y ACTIVOS FIJOS EN SISTEMAS HOSPITALARIOS

---

## 1.5 Protocolos de comunicación

EPCGlobal, consorcio de empresas específicamente orientada a desarrollar estándares globales para un Código Electrónico de Producto (EPC, por sus siglas en inglés), tiene el objetivo de normalizar la información contenida en las etiquetas RFID. Para ello cuenta con una cantidad de protocolos que permiten la comunicación entre el lector y las etiquetas, perteneciente a este estándar se encuentra el Protocolo de Lectura a Bajo Nivel (LLRP, por sus siglas en inglés).

El LLRP facilita la gestión de dispositivos lectores, mitigando las interferencias lector-etiqueta y lector-lector, y maximiza la eficiencia de señalización y operaciones con datos sobre las etiquetas. LLRP soporta el protocolo aire (*Air Protocol*) Ultra Alta Frecuencia Clase-1 Generación-2 (UHF C1G2, por sus siglas en inglés), estándar que fue desarrollado por la EPCglobal para estandarizar el protocolo de interfaz aire vía radiofrecuencia entre las etiquetas y los lectores RFID.

El *Air Protocol* define los requerimientos físicos y lógicos para la comunicación entre las etiquetas y los lectores RFID. Específicamente este protocolo define la capa de señal en la comunicación entre la etiqueta y el lector RFID, así como las operaciones de procedimientos y órdenes entre los mismos. LLRP provee el control de todas las funcionalidades bases de cualquier lector que use el *Air-ProtocolUHF C1G2*, incluyendo el acceso a la configuración de bajo nivel del mismo.

Este estándar permite que los productores de lectores en vez de tener que crear un protocolo propietario para adicionarle nuevas funcionalidades a un lector, puedan desarrollar extensiones sobre este mismo protocolo, haciendo uso de un marco de trabajo que brinda el propio LLRP (18).

## 1.6 Sistemas de identificación por radiofrecuencia integrados a los procesos de control de acceso y activos fijos

El sector salud requiere de instrumentos que le permitan desempeñar su labor de forma más eficaz. Muchos de los métodos que son usados actualmente para la administración de sus recursos no resultan eficientes debido a la gran demanda de servicios y las pocas soluciones escalables con las que cuentan. Hoy en día los hospitales enfrentan el reto de implementar tecnologías que les permita ofrecer servicios de mayor calidad, y operar con mayores niveles de eficiencia que reduzcan tiempo, recursos y errores en los procesos. La tecnología RFID es una solución a estos problemas. Actualmente en el mundo, muchos hospitales usan esta tecnología para mejorar la atención en los centros de salud. Para ello es importante

# CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA- METODOLOGICA DEL CONTROL DE ACCESO Y ACTIVOS FIJOS EN SISTEMAS HOSPITALARIOS

---

analizar las posibles ventajas y desventajas en la aplicación de esta tecnología dado que es relativamente nueva y surgen dudas sobre diversos elementos tecnológicos y su uso. A pesar de lo mencionado anteriormente muchos son los beneficios ya obtenidos actualmente, entre los que destacan la monitorización de pacientes y el control de sus activos fijos.

## **Sistemas internacionales**

A continuación se mencionan algunos de los principales sistemas informáticos que en el mundo se encuentran destinados al control de acceso y seguimiento de activos fijos haciendo uso de la tecnología RFID, con el objetivo de encontrar soluciones factibles a los problemas planteados describiendo de cada uno sus principales ventajas y desventajas.

### **Sistema ASETRAC20**

#### **País: Estados Unidos**

Desarrollado con el objetivo de reducir los costes de pérdidas de equipamiento hospitalario y las pérdidas de tiempo del personal dedicado a las búsquedas del equipamiento extraviado. Para ello se fijaron etiquetas RFID al equipamiento, para hacer saltar una alarma siempre que un determinado equipo saliera de su perímetro asignado. El sistema ASETRAC dispone de una interfaz gráfica donde se pueden mostrar planos del lugar de despliegue, ayudando así al personal en el seguimiento de los equipos (19).

Este sistema fue rechazado como posible cumplimiento del objetivo propuesto, por las siguientes razones:

- Sistema monoplataforma y está implementado con tecnología propietaria.
- Para su funcionamiento es necesario un equipo con características especiales en el hardware debido a la interfaz gráfica que muestra.

### **Sistema iRISupplyTM**

#### **País: Estados Unidos**

Desarrollado por Mobile Aspects, utiliza una arquitectura de seguimiento RFID para automatizar la gestión de inventario, el control de la caducidad de los dispositivos, y otros procesos operacionales claves en el cuidado de los pacientes (20).

Este sistema fue rechazado como posible cumplimiento del objetivo propuesto, por las siguientes razones:

# CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA- METODOLOGICA DEL CONTROL DE ACCESO Y ACTIVOS FIJOS EN SISTEMAS HOSPITALARIOS

---

- No gestiona toda la información relacionada con los reportes estadísticos sobre pérdidas de los recursos en la entidad.
- La información que presenta es estática o sea no aprovecha todos los beneficios que brinda la tecnología RFID.

## **Sistema AXESS**

### **País: Estados Unidos**

Solución integral, de altas prestaciones técnicas y fácil funcionamiento, para sistemas de control y gestión del flujo de acceso a ferias, congresos, complejos deportivos, edificios corporativos y grandes eventos. El usuario está acreditado con una tarjeta RFID que al ser detectada por la antena valida el permiso del usuario al local (21).

Este sistema fue rechazado como posible cumplimiento del objetivo propuesto, por las siguientes razones:

- Sistemadiseñado únicamente para dispositivos táctiles.
- No permite modificar la información una vez entrada al sistema.
- Está desarrollado con base a las necesidades tan particulares y complejas de países específicos del primer mundo.

Como resultado del estudio realizado se pudieron identificar los principales sistemas internacionales que hacen uso de la tecnología RFID en los procesos de control de acceso y activos fijos, lográndose definir las principales funcionalidades de estos productos y características específicas de los mismos, así como debilidades y fortalezas. También se comprobó la necesidad de aplicar esta tecnología al Sistema de Información Hospitalaria xavia HIS ya que le proporcionaría potencialidades a la hora de comercializarlo.

### **1.7 Patrones y lenguajes utilizados**

Establecer con precisión las herramientas a utilizar para llevar el desarrollo de una aplicación resulta de carácter significativo, ya que permite trabajar de forma organizada, así como obtener una solución satisfactoria del problema a resolver.

#### **1.7.1 Capa de presentación**

## CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA- METODOLOGICA DEL CONTROL DE ACCESO Y ACTIVOS FIJOS EN SISTEMAS HOSPITALARIOS

---

Esta capa proporciona la interfaz visual que los clientes utilizarán para ver la información y los datos. En este nivel, los componentes son responsables de solicitar y recibir servicios de otros componentes del mismo nivel o del nivel de servicios de negocio.

- **Java Server Faces**

*Java Server Faces* (JSF, por sus siglas en inglés) es un *framework* para aplicaciones Java basadas en web que permitió la simplificación en el desarrollo de interfaces de usuario en aplicaciones Java EE. JSF usa *Facelets* como la tecnología para hacer el despliegue de las páginas, pero también se puede acomodar a otras tecnologías como XUL (22).

Es muy flexible, permitiendo incluso crear componentes informáticos personalizados. Resuelve los problemas de duplicidad al pulsar un botón dos veces y posee gran cantidad de implementaciones. El uso de JSF permite el manejo de estados y eventos, la asociación entre los datos de la interfaz y los datos de la aplicación web, la especificación de la navegación del usuario, entre otras funcionalidades.

- **Facelets**

Es un *framework* web de código abierto bajo la licencia Apache y tecnología alternativa de controlador de vista de JSF. *Facelets* soporta todos los componentes informáticos de interfaz de usuario JSF y construye su propio árbol de componente informáticos, lo que refleja el punto de vista de una aplicación de este tipo. El mismo, permite que *Java Server Pages* (JSP, por sus siglas en inglés) y JSF puedan funcionar conjuntamente en una misma aplicación web. Además, su trabajo está basado en plantillas y tiene una fácil composición de componentes informáticos. Incluye funciones para expresiones, así como también permite la creación de librerías de componente informáticos. *Facelets* permite en general el desarrollo amigable para el diseñador gráfico (23).

- **Ajax4jsf**

Ajax4jsf es una librería de código abierto que se integra totalmente en la implementación de JSF, y extiende la funcionalidad de sus etiquetas, dotándolas con tecnología Ajax sin código JavaScript. Mediante este *framework* se puede variar el ciclo de vida de una petición JSF, recargar determinados componente informáticos de la página sin necesidad de refrescarla en su totalidad, realizar peticiones al servidor de forma automática, controlar cualquier evento de usuario, entre otros (24).

# CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA- METODOLOGICA DEL CONTROL DE ACCESO Y ACTIVOS FIJOS EN SISTEMAS HOSPITALARIOS

---

- **RichFaces**

Es una librería de componente informáticos ricos para JSF, y además posee un *framework* avanzado para la integración sencilla de las funcionalidades Ajax dentro del desarrollo de las aplicaciones del negocio. Es capaz de trabajar con cualquier implementación de JSF y con la mayoría de sus bibliotecas de componente informáticos sin ninguna configuración adicional. Además, permite crear interfaces de usuario modernas de manera eficiente y rápida, basadas en componentes informáticos altamente configurables en cuanto a temas y esquemas de colores predefinidos por el propio *framework* o desarrollados a conveniencia (25).

## 1.7.2 Capa de negocio

En esta capa residen los programas que se ejecutan, se reciben las peticiones del usuario y se envían las respuestas tras el proceso. Se establecen todas las reglas que deben cumplirse. Es la encargada de comunicarse con la capa de presentación, para recibir las solicitudes y presentar los resultados, y con la capa de datos, para solicitar al gestor de base de datos el almacenamiento o recuperación de datos.

- **Enterprise JavaBeans**

Los EJB son una de las Interfaces de Programación de Aplicaciones (API, por sus siglas en inglés). Estos proporcionan un modelo de componente informáticos distribuido estándar del lado del servidor. Su objetivo es dotar al programador de un modelo que le permita abstraerse de los problemas generales de una aplicación (conurrencia, transacciones, persistencia, seguridad, entre otros), para centrarse en el desarrollo de la lógica de negocio en sí. La ventaja de estar basado en componentes informáticos permite que éstos sean flexibles y sobre todo reutilizables. Las aplicaciones que utilizan la arquitectura *Enterprise JavaBeans* son escalables, transaccionales y de multiusuario seguro. Estas aplicaciones se pueden escribir una vez, y luego desplegar en cualquier plataforma de servidor capaz de soportar la especificación de *Enterprise JavaBeans* (26).

## 1.7.3 Capa de datos

La capa de acceso a datos contiene principalmente las tecnologías utilizadas para acceder y persistir los datos. Se encuentra conformada por uno o más gestores de bases de datos encargados de almacenar, recibir y recuperar la información a través de los componentes agrupados en la misma.

# CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA- METODOLOGICA DEL CONTROL DE ACCESO Y ACTIVOS FIJOS EN SISTEMAS HOSPITALARIOS

---

- **Java Persistence**

Es la API de persistencia desarrollada para la plataforma Java EE y está incluida en el estándar EJB3. Esta API busca unificar la manera en que funcionan las utilidades que provee un mapeo objeto-relacional. El objetivo que persigue su diseño es no perder las ventajas de la orientación a objetos al interactuar con una base de datos, como sucedía con EJB2, y permitir usar objetos regulares conocidos como *Plain Old Java Object* (POJOs, por sus siglas en inglés).

- **Hibernate**

Es una herramienta de mapeo objeto-relacional para la plataforma Java, que facilita el mapeo de atributos entre una base de datos relacional tradicional y el modelo de objetos de una aplicación mediante archivos declarativos XML. Cuenta con el *Hibernate Query Language* (HQL, por sus siglas en inglés) que es un lenguaje de consulta similar al SQL. Además brinda, de una manera muy rápida y mejorada, la posibilidad de generar bases de datos en cualquiera de los entornos soportados: PostgreSQL, Oracle, DB2, MySql, entre otros, además de ser una herramienta de código abierto (27).

## 1.7.4 Lenguajes

Una vez analizados los lenguajes de programación se indican a continuación los utilizados para dar solución a la problemática propuesta.

- **Java 1.6**

Lenguaje de programación desarrollado por la compañía *Sun Microsystems*, que utiliza el paradigma de la Programación Orientada a Objetos (POO, por sus siglas en inglés). Es un lenguaje robusto pues no permite el manejo directo del hardware ni de la memoria. Dentro de sus principales ventajas se encuentra la de ser multiplataforma. Con Java se pueden programar aplicaciones webs dinámicas, con acceso a bases de datos, utilizando XML, con cualquier tipo de conexión de red entre cualquier sistema. Este lenguaje es utilizado de manera horizontal en el desarrollo del sistema, pues puede estar presente en las diferentes capas de la aplicación (28).

La plataforma Java consta de las siguientes partes:

- El lenguaje de programación, Java.
- La máquina virtual de Java o JRE, que permite la portabilidad en ejecución.
- El API Java, una biblioteca estándar para el lenguaje.

- **Lenguaje de Marcado de Hipertexto Extensible**

XHTML es una versión más estricta y clara de HTML, que elimina sus limitaciones de uso con herramientas basadas en XML. Su objetivo es avanzar de tal forma que se pueda lograr una web semántica, donde la información y la forma de presentarla estén claramente separadas. Es el lenguaje de marcas por defecto que utiliza JSF.

## **1.8 Guía de desarrollo de Software**

El *Capability Maturity Model Integration* (CMMI, por sus siglas en inglés) es un modelo para la mejora de los procesos de desarrollo, adquisición, y mantenimiento de productos y servicios. Las mejores prácticas de CMMI se publican en documentos denominados modelos, los cuales proponen un conjunto de prácticas que las organizaciones pueden adoptar para implantar procesos productivos más efectivos.

CMMI establece una medida del progreso y plantea que las organizaciones pueden ubicarse en alguno de cinco posibles niveles de madurez, dependiendo del grado de sofisticación de sus procesos, este enfoque se denomina “Representación Escalonada”. Cada nivel de madurez, con excepción del inicial, queda caracterizado por un conjunto de áreas de proceso que agrupan prácticas que, al ser ejecutadas colectivamente, permiten cumplir con algún objetivo que es considerado importante para el modelo.

CMMI consta de 22 áreas de proceso distribuidas dentro de 5 niveles de madurez:

- ✓ Nivel 1: Inicial.
- ✓ Nivel 2: Administrado.
- ✓ Nivel 3: Definido.
- ✓ Nivel 4: Cuantitativamente administrado.
- ✓ Nivel 5: Optimizado.

Como resultado del programa de mejora en el cual estuvo inmersa la Universidad de las Ciencias Informáticas y que concluyó con la certificación internacional del nivel 2 de CMMI, se obtuvo una guía para el proceso de desarrollo de software. Las áreas de procesos que lo forman son:

- ✓ Administración de Requisitos (REQM).
- ✓ Planeación del Proyecto (PP).
- ✓ Monitoreo y Control del Proyecto (PMC).

# CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA- METODOLOGICA DEL CONTROL DE ACCESO Y ACTIVOS FIJOS EN SISTEMAS HOSPITALARIOS

---

- ✓ Medición y Análisis (MA).
- ✓ Aseguramiento de la Calidad de Procesos y productos (PPQA).
- ✓ Administración de la Configuración (CM).
- ✓ Administración de Acuerdos con Proveedores (SAM).

- **Lenguaje Unificado de Modelado**

Lenguaje Unificado de Modelado (UML, por sus siglas en inglés) es un lenguaje para visualizar, especificar, construir y documentar los artefactos de un sistema que involucra una gran cantidad de software. Permite modelar sistemas con tecnología orientada a objetos. UML ofrece un estándar para describir un plano del modelo e incluye aspectos conceptuales tales como: procesos de negocios y funciones del sistema.

Dentro de sus características se pueden mencionar algunas tales como:

- Tecnología orientada a objetos.
- Viabilidad en la corrección de errores.
- Desarrollo iterativo e incremental.
- Participación del cliente en todas las etapas del proyecto.

## **1.9 Herramientas y tecnologías utilizadas para la solución**

Es importante apoyarse en herramientas y tecnologías que faciliten las tareas una vez que se cuente con una guía de desarrollo adecuada. Seguidamente se describen las aplicaciones seleccionadas para dar solución a la problemática planteada.

- **Java Enterprise Edition 5**

Esta tecnología permite al desarrollador crear una aplicación de empresa portable entre plataformas y escalable, a la vez que se integra con tecnologías anteriores. Otros beneficios añadidos son, por ejemplo, que el servidor de aplicaciones puede manejar transacciones, la seguridad, escalabilidad, concurrencia y gestión de los componente informáticos desplegados, significando que los desarrolladores pueden concentrarse más en la lógica de negocio de los componente informáticos en lugar de en tareas de mantenimiento de bajo nivel (29).

- **JBoss Seam 2.1**

## CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA- METODOLOGICA DEL CONTROL DE ACCESO Y ACTIVOS FIJOS EN SISTEMAS HOSPITALARIOS

---

Es un *framework* para el desarrollo de aplicaciones web en Java, que define un modelo de componente informáticos uniforme para toda la lógica de negocio de las aplicaciones que sean desarrolladas mediante su utilización. La misma integra tecnologías como Ajax, JSF, *Java Persistence* (JPA, por sus siglas en inglés), *Enterprise Java Beans* (EJB, por sus siglas en inglés) y *Business Process Management* (BPM, por sus siglas en inglés) en un sistema unificado con sofisticadas herramientas (30).

Automatiza muchas de las tareas comunes y hace un uso extensivo de las anotaciones para poder reducir la cantidad de código XML que es necesario escribir, reduce de manera importante la cantidad total de codificación necesaria. Permite la creación de complejas aplicaciones Web.

- **JBoss Application Server 4.2.2**

*JBoss Application Server* es el servidor de aplicaciones de código abierto más usado en el mercado. Se encuentra bajo la licencia GNULGPL, por lo que puede libremente usarse sin costo alguno en cualquier aplicación comercial o ser redistribuido. Por ser una plataforma certificada JEE 5, soporta todas las especificaciones correspondientes, incluyendo servicios adicionales como *clustering*, *caching* y persistencia.

Es el más recomendado para aplicaciones Java, pues está basado en este lenguaje de programación, y también es propicio para aplicaciones basadas en la web. También soporta *Enterprise Java Beans* 3.0 (EJB) (31).

- **PostgreSQL 8.4**

PostgreSQL es un sistema gestor de base de datos (SGBD) que ofrece una potencia adicional al incorporar los conceptos de clases, herencia, tipos y funciones; de modo que los usuarios puedan extender fácilmente el sistema. Utiliza un modelo cliente/servidor y usa multiprocesos en vez de multihilos para garantizar la estabilidad del sistema. PostgreSQL incluye reglas, restricciones, disparadores y una integridad transaccional que le aportan flexibilidad y potencia. Estas características incorporan a este gestor en la categoría de las bases de datos identificadas como objeto-relacionales. Se destaca por su robustez, escalabilidad y cumplimiento de los estándares SQL. Es un software de código abierto que está bajo la licencia *Berkeley Software Distribution* (BSD, por sus siglas en inglés) (32).

- **Eclipse 3.5**

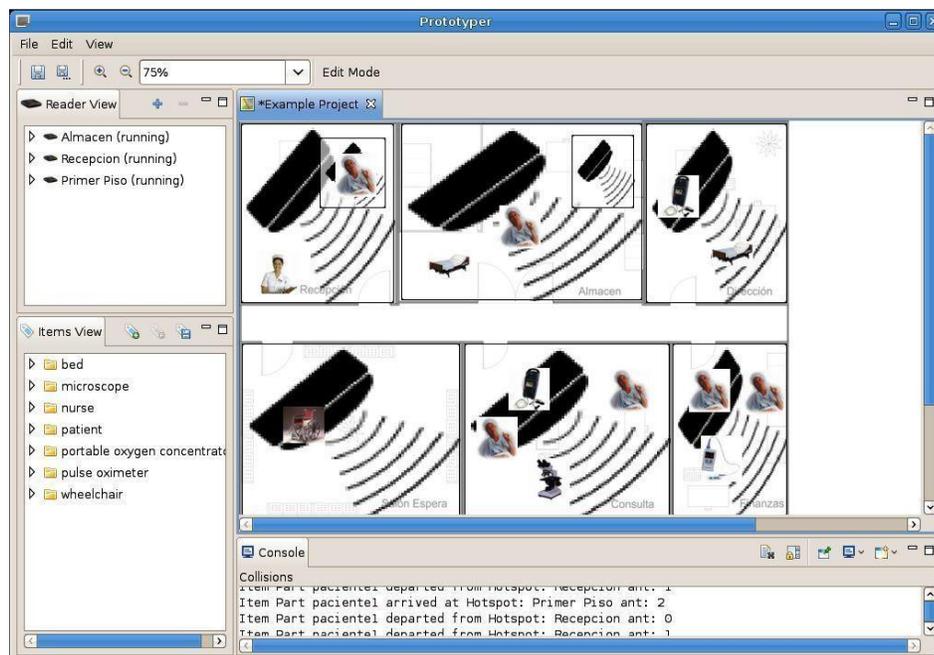
## CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA- METODOLOGICA DEL CONTROL DE ACCESO Y ACTIVOS FIJOS EN SISTEMAS HOSPITALARIOS

Esta herramienta es un Entorno Integrado de Desarrollo (IDE, por sus siglas en inglés) multiplataforma, de código abierto y extensible. Ofrece la posibilidad de añadirle módulos o pluggins, que facilita el uso de JBoss Tools, para el desarrollo de aplicaciones con *RichFaces*, *Seam*, *Hibernate* y el JBoss AS. Además, brinda cobertura a otros lenguajes de programación aparte de Java, como pueden ser C/C++, Python, Cobol, Fortran, PHP, entre otros (33).

- **Simulador Rifi di Prototyper 1.0**

*Rifi di Prototyper 1.0* es una herramienta de demostración basada en un emulador RFID. Permite gestionar los lectores y ubicarlos dentro de un modelo o esquema de una entidad, además pueden ser creados diversos artículos los cuales pueden ser introducidos dentro o fuera del rango del lector. Este simulador permite poner a prueba los flujos de la entidad y la lógica empresarial con bastante facilidad (34).

A continuación se muestra en la figura 1.12 el uso de la herramienta en funcionamiento para tener un mejor entendimiento de sus características.



**Figura 1.12. Simulador Rifi di Prototyper**  
Fuente: elaboración propia

- **iReport**

Es un constructor y diseñador visual de informes, poderoso, intuitivo y fácil de usar para *JasperReports* escrito en Java. Este instrumento permite que los usuarios corrijan visualmente informes complejos con

## CAPÍTULO 1. FUNDAMENTACIÓN TEÓRICA- METODOLOGICA DEL CONTROL DE ACCESO Y ACTIVOS FIJOS EN SISTEMAS HOSPITALARIOS

---

cartas, imágenes y sub informes. iReport está además integrado con *JFreeChart*, una de las bibliotecas gráficas *Open Source* más difundidas para Java. Escrito en el lenguaje java y gratuito. Incluye asistentes para crear automáticamente informes, generar los sub reportes y las plantillas, además de soportar la internacionalización nativamente (35).

- **pgAdmin 3.0**

Su interfaz gráfica soporta todas las características de PostgreSQL y permite que la administración sea mucho más sencilla. Es la más completa y popular con licencia *Open Source*. Está escrita en C++. Usa la librería gráfica multiplataforma *wxWidgets*, lo que permite que se pueda usar en Linux, FreeBSD, Solaris, Mac OS X y Windows. La aplicación incluye también un editor SQL con resaltado de sintaxis, un editor de código en el servidor, un agente para lanzar script programados y mucho más. La conexión al servidor puede hacerse mediante conexión TCP/IP o Unix Domain Sockets, y puede encriptarse mediante Capa de Conexión Segura (SSL) para mayor seguridad (36).

- **Visual Paradigm 6.4**

Esta herramienta facilita el diseño y visualización de elementos de software, para ello utiliza UML y ofrece una gama de facilidades para el modelado de aplicaciones. Está orientada a la creación de diseños usando el paradigma de programación orientada a objetos. Provee soporte para la generación de código, permite dibujar todos los tipos de diagramas de clases, código inverso, generar código desde diagramas y generar documentación. Soporta el ciclo de vida completo del desarrollo de software: análisis y diseño orientados a objetos, construcción, pruebas y despliegue (37).

En este capítulo se presentaron y estudiaron los sistemas existentes relacionados con el tema de la investigación, así como conceptos importantes que facilitan aún más la comprensión de toda la investigación realizada, además de las tecnologías, metodologías, herramientas y lenguajes que se usarán para el desarrollo del sistema propuesto. Estos aspectos proveen la base de conocimientos necesaria para llevar a cabo la elaboración del sistema.

### Capítulo 2. Diseño del sistema para el control de acceso y activos fijos

Este capítulo describe las características generales del sistema y la propuesta de solución. Además se describe el Modelo de Negocio y se especifican los requisitos funcionales y no funcionales del sistema. Se construyen los diagramas de clases del diseño y para una mayor comprensión de éste se realiza la descripción de sus clases. Se explica la arquitectura utilizada y los principales patrones de diseño usados.

El modelado de procesos de negocio es la base para comprender mejor la operación de una organización, documentar y publicar los procesos buscando una estandarización en la misma. Un proceso de negocio es una serie de actividades diseñadas para producir una salida específica para un cliente o mercado particular. Presenta un orden lógico y específico de las actividades de trabajo a través del tiempo y el espacio, cuenta con un comienzo, un fin, así como entradas y salidas bien identificadas.

Una vez analizado los procesos del negocio se procede a realizar el modelado del mismo obteniendo así los actores y sus respectivas funciones, así como la descripción de dichos procesos.

#### 2.1 Actores del negocio

A partir del modelado de los procesos existentes en el negocio se concibió la relación de los actores relacionados en el mismo así como los objetivos específicos de forma individual.

**Tabla 2.1. Actores del negocio**

Actor	Objetivo
Contador General de AF	Manipula todas las funcionalidades del módulo de Activo Fijo del Departamento de Contabilidad.
Técnico	Es el encargado de realizar las operaciones específicas de restricción con el personal y los activos.
Director de Contabilidad y Finanzas	Además de ser el encargado de realizar las funciones como Director de Contabilidad y Finanzas, revisa y aprueba los documentos y expedientes referentes a los Activos Fijos dentro del departamento de Contabilidad y Finanzas.
Jefe de Almacén	Es el encargado de realizar todas las operaciones referentes al almacén de los activos fijos tangibles en la entidad.
Especialista Superior de Inventario	Es el encargado de la conformación del inventario personalizado de cada uno de los activos que se gestionen en la entidad.

### 2.2 Descripción de los procesos del negocio

A continuación se presenta los procesos de mayor importancia existentes en el negocio, una breve descripción de los mismos, así como el diagrama de proceso del negocio perteneciente a cada uno de ellos. Se recomienda ver el fichero del modelo de proceso de negocio que se encuentra en el expediente de proyecto para un mayor entendimiento.

- ✓ Creación de áreas en la entidad: proceso encargado de la gestión de cada una de las áreas de la entidad ya sea para adicionarlas, modificarlas, eliminarlas o buscarlas.

La figura 2.1 muestra el diagrama de proceso de negocio creación de áreas en la entidad, mostrando los actores, actividades y relaciones entre ellas existentes.

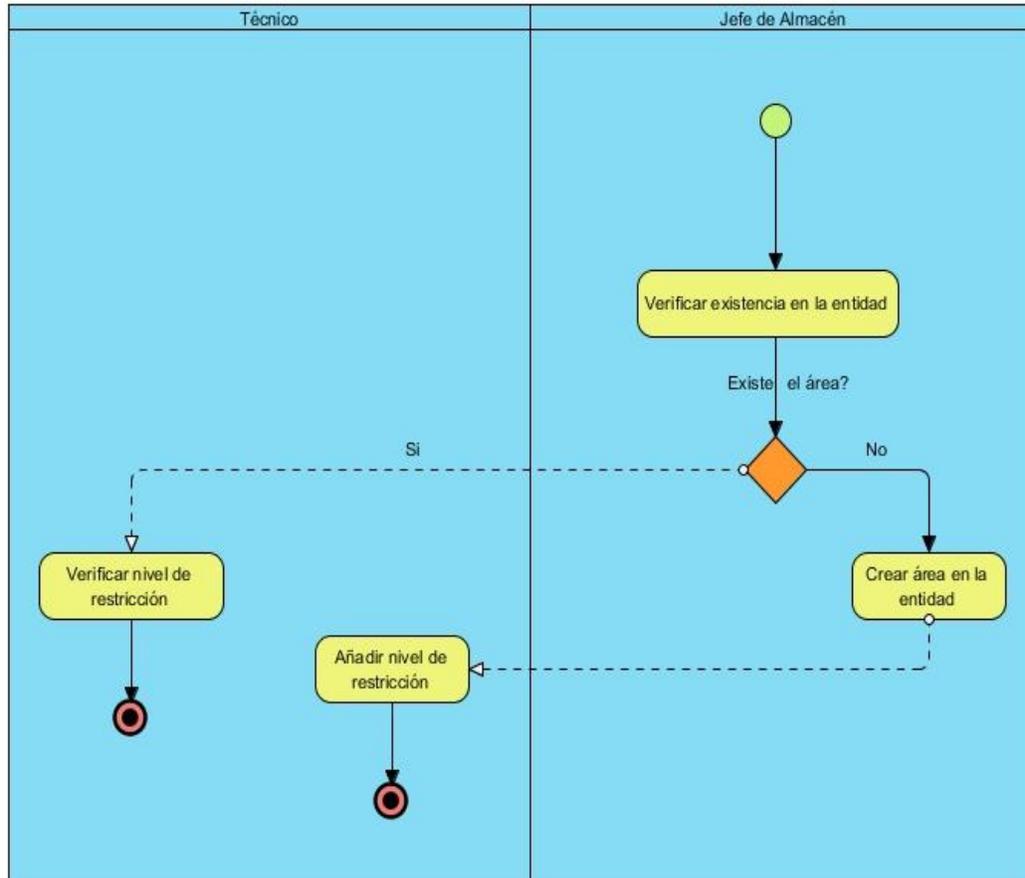


Figura 2.1. DCA Creación de áreas en la entidad

Fuente: Elaboración propia

## CAPÍTULO 2. DISEÑO DEL SISTEMA PARA EL CONTROL DE ACCESO Y ACTIVOS FIJOS

- ✓ Ingreso de activos fijos tangibles (AFT): da lugar a toda la actividad referente a los activos fijos tangibles que se presente en la entidad, dígame adicionarlos a la misma, eliminarlos en caso de desuso o presencia de algún fallo, modificaciones o búsqueda de los mismos.

La figura 2.2 muestra el diagrama de proceso de negocio ingreso de activos fijos tangibles a la entidad, mostrando los actores, actividades y relaciones entre ellas existentes.

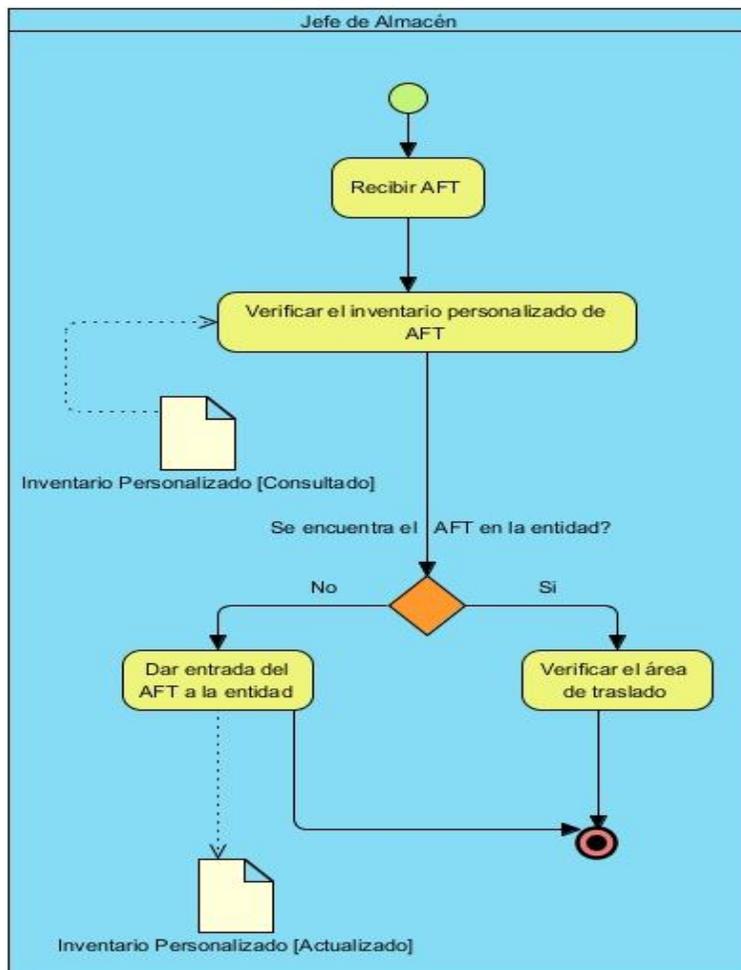


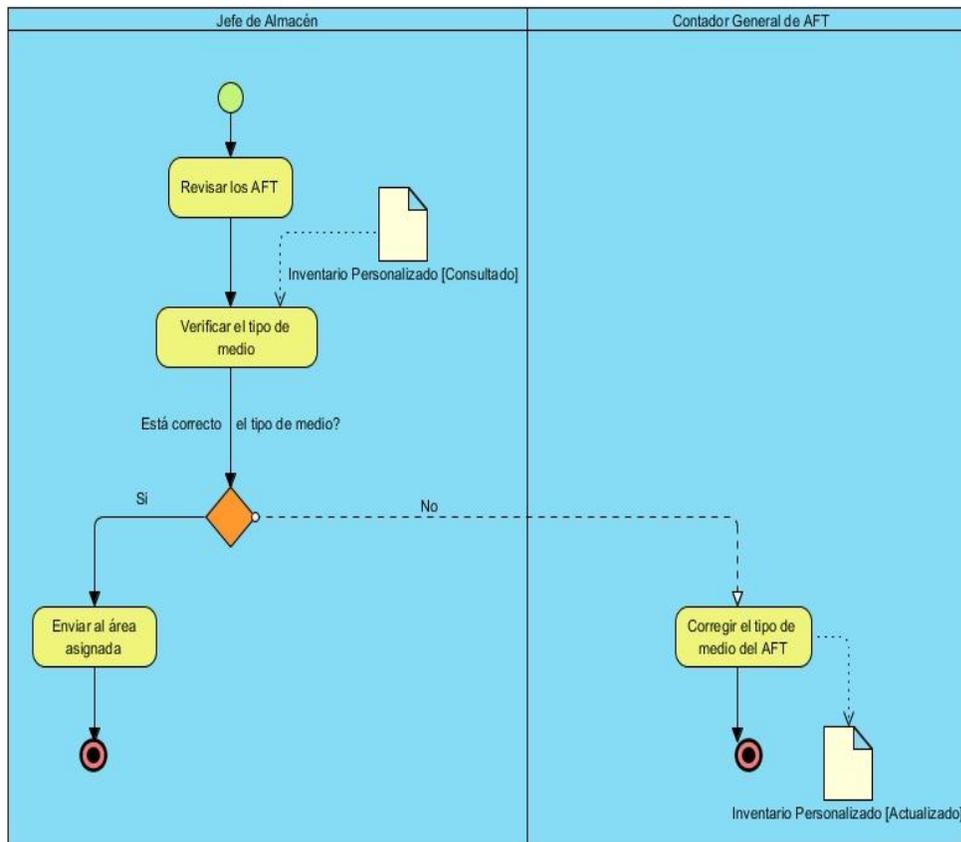
Figura 2.2. DCA Ingreso de activos fijos tangibles

Fuente: Elaboración propia

- ✓ Tipos de medios: se procede una vez que el activo sea gestionado a clasificarlos según el tipo de medio.

## CAPÍTULO 2. DISEÑO DEL SISTEMA PARA EL CONTROL DE ACCESO Y ACTIVOS FIJOS

La figura 2.3 muestra el diagrama de proceso de negocio ingreso de activos fijos tangibles a la entidad, mostrando los actores, actividades y relaciones entre ellas existentes.

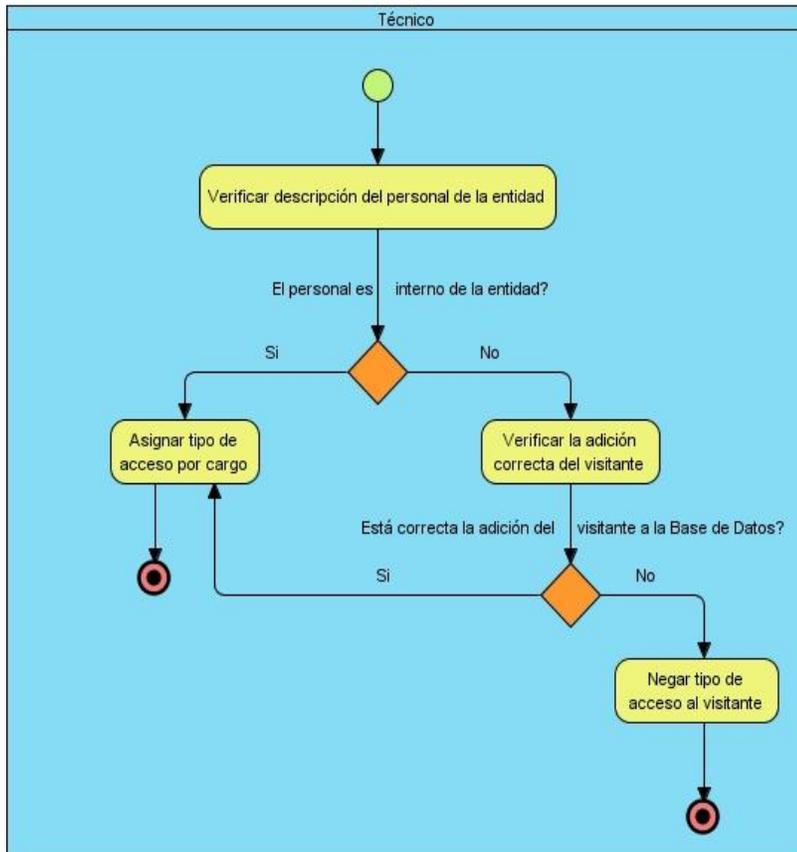


**Figura 2.3. DCA Tipos de medios**

**Fuente: Elaboración propia**

- ✓ Tipo de acceso al personal: proceso que se realiza con el objetivo de que todo el personal tanto interno como externo de la entidad tenga acceso sólo a las áreas que lo requieran.

La figura 2.4 muestra el diagrama de proceso de negocio tipo de acceso al personal, mostrando los actores, actividades y relaciones entre ellas existentes.



**Figura 2.4. DCA Tipo de acceso al personal**

**Fuente: Elaboración propia**

### 2.3 Propuesta del sistema

El sistema que se desarrollará tiene como objetivo llevar un control sobre los activos fijos existentes en una entidad sanitaria, así como controlar el acceso a las diferentes áreas que permita:

- ✓ La gestión de las diversas áreas de la entidad así como de los activos fijos tangibles en la misma.
- ✓ La gestión de los tipos de medios de los activos fijos tangibles para la creación del inventario personalizado a partir de la entrada de cada uno de los mismos.
- ✓ La gestión del traslado de los activos fijos dentro de la entidad.
- ✓ La gestión del personal interno y externo de la entidad.
- ✓ La gestión de las etiquetas tanto al personal interno como externo de la entidad y a los activos fijos tangibles.
- ✓ La gestión del nivel de restricción y tipo de acceso para el personal en la entidad.
- ✓ La gestión de los lectores o antenas en cada una de las áreas o departamento de la entidad.

### 2.4 Especificación de los requisitos de software

Los requerimientos para un sistema son la descripción de los servicios proporcionados por el sistema y sus restricciones operativas, estos reflejan las necesidades de los clientes de un sistema que ayude a resolver algún problema (38).

Para el correcto funcionamiento del sistema informático se especificaron los requerimientos funcionales y no funcionales que el sistema debe cumplir.

#### 2.4.1 Requisitos funcionales

A partir del análisis del modelado de los procesos del negocio y las actividades a automatizar se establecen las funcionalidades con que el sistema debe contar para dar solución al problema identificado.

Los requerimientos funcionales son capacidades o condiciones que el sistema debe cumplir. Estos detallan las funcionalidades o servicios que se espera que el sistema cumpla para satisfacer las necesidades del usuario y define el comportamiento del sistema, sin tomar en consideración ningún tipo de restricción física, de manera que se conservan invariables (39).

A continuación se muestra la relación de requisitos funcionales obtenidos luego del análisis del modelo de proceso de negocio:

#### RF1- Gestionar áreas

**RF1.1 - Adicionar áreas:** se adicionan las áreas necesarias a una entidad sanitaria.

**RF1.2 - Eliminar áreas:** se eliminan las áreas en caso de error o desuso de una entidad sanitaria.

**RF1.3 - Buscar áreas:** se buscan las áreas necesarias de una entidad sanitaria.

**RF1.4 - Modificar áreas:** se modifican las áreas en caso de error en una entidad sanitaria.

#### RF2 - Gestionar AFT

**RF2.1 - Adicionar AFT:** se adicionan los activos fijos tangibles necesarios en una entidad sanitaria.

**RF2.2 - Eliminar AFT:** se eliminan los activos fijos tangibles en caso de error o desuso en una entidad sanitaria.

**RF2.3 - Buscar AFT:** se buscan los activos fijos tangibles necesarios en una entidad sanitaria.

**RF2.4 - Modificar AFT:** se modifican los activos fijos tangibles en caso de error en una entidad sanitaria.

### **RF3 - Gestionar tipos de medios**

**RF3.1 - Adicionar tipos de medios:** se adicionan los tipos de medios a los activos fijos tangibles necesarios en una entidad sanitaria.

**RF3.2 - Eliminar tipos de medios:** se eliminan los tipos de medios a los activos fijos tangibles en caso de error o desuso en una entidad sanitaria.

**RF3.3 - Buscar tipos de medios:** se buscan los tipos de medios de los activos fijos tangibles necesarios en una entidad sanitaria.

**RF3.4 - Modificar tipos de medios:** se modifican los tipos de medios de los activos fijos tangibles en caso de error en una entidad sanitaria.

**RF4 - Traslados internos de AFT:** se registran los traslados que se realicen a un activo fijo tangible dentro de la entidad sanitaria.

### **RF5 - Gestionar nivel restricción por área**

**RF5.1 - Adicionar nivel restricción:** se adiciona un nivel de restricción a cada una de las áreas correspondientes a la entidad para controlar el acceso a las mismas.

**RF5.2 - Eliminar nivel restricción:** se elimina un nivel de restricción de un área correspondiente a la entidad en caso de error o desuso.

**RF5.3 - Buscar nivel restricción:** se busca un nivel de restricción de un área correspondiente a la entidad para controlar el acceso a las mismas.

**RF5.4 - Modificar nivel restricción:** se modifica un nivel de restricción de un área correspondiente a la entidad en caso de existir algún error.

### **RF6 -. Gestionar personal interno**

**RF6.1 - Adicionar personal interno:** se adiciona el personal interno a la entidad sanitaria con el objetivo de acceder a las áreas de dicha institución.

**RF6.2 - Eliminar personal interno:** se elimina el personal interno de la entidad sanitaria en caso de ocurrir algún error al ser agregado.

**RF6.3 - Buscar personal interno:** se busca el personal interno a la entidad sanitaria.

**RF6.4 - Modificar personal interno:** se modifica el personal interno de la entidad sanitaria en caso de ocurrir algún error al ser agregado.

### **RF7 - Gestionar personal externo**

## CAPÍTULO 2. DISEÑO DEL SISTEMA PARA EL CONTROL DE ACCESO Y ACTIVOS FIJOS

---

**RF7.1 – Adicionar personal externo:** se adiciona el personal externo a la entidad sanitaria con el objetivo de acceder a dicha institución.

**RF7.2 - Eliminar personal externo:** se elimina el personal externo de la entidad sanitaria en caso de ocurrir algún error al ser agregado.

**RF7.3 - Buscar personal externo:** se busca el personal externo a la entidad sanitaria.

**RF7.4 - Modificar personal externo:** se modifica el personal externo de la entidad sanitaria en caso de ocurrir algún error al ser agregado.

**RF8 –Quitar acceso al personal:** se le asigna el tipo de acceso que tendrá el personal interno de la entidad sanitaria en dependencia de sus responsabilidades.

**RF8.1 - Buscar personal:** se busca el personal interno de la entidad sanitaria para verificar el tipo de acceso del mismo.

### **RF9 - Gestionar tipo de acceso**

**RF9.1 - Adicionar tipo de acceso:** se adiciona el tipo de acceso que tendrá una persona en correspondencia con las responsabilidades y cargos que presente.

**RF9.2 - Modificar tipo de acceso:** se modifica el tipo de acceso que tendrá una persona en correspondencia con las responsabilidades y cargos que presente en caso de existir algún error.

**RF9.3 - Eliminar tipo de acceso:** se elimina el tipo de acceso que tendrá una persona en correspondencia con las responsabilidades y cargos que presente en caso de existir algún error o no sea utilizado en la entidad.

**RF10 -Cambiar estado del activo:** se le cambiará el estado al AFT a ocioso en caso de que ya no se utilice en la entidad o activo en caso de que se comience su uso nuevamente.

### **RF11 - Gestionar antena**

**RF11.1 - Adicionar antena:** se adicionan antenas a la entidad sanitaria.

**RF11.2 - Buscar antena:** se busca una antena que haya sido agregada a la entidad sanitaria.

**RF11.3 - Eliminar antena:** se elimina una antena que haya sido agregada con anterioridad a la entidad sanitaria y que en la cual exista algún error o esté en desuso.

**RF11.4 - Modificar antena:** se modifica una antena que haya sido agregada con anterioridad a la entidad sanitaria y que en la cual exista algún error o esté en desuso.

## CAPÍTULO 2. DISEÑO DEL SISTEMA PARA EL CONTROL DE ACCESO Y ACTIVOS FIJOS

---

**RF12 - Monitorización de acceso por áreas:** se realiza una monitorización de las áreas para controlar el acceso a las mismas.

**RF13 - Monitorización de AFT por áreas:** se realiza una monitorización de los activos fijos tangibles para controlar su ubicación y que no sean trasladados sin autorización del área perteneciente.

**RF14 - Gestionar lector:** se administran todos los lectores que serán utilizados para mantener un control sobre las antenas en dicha entidad.

**RF15- Reporte personalizado de inventario:** se realiza un reporte que guarde toda la información de los activos presentes en la entidad.

**RF16 – Reporte personalizado de violaciones por acceso:** se realiza un reporte que guarda todas las violaciones que han ocurrido en las áreas de la entidad por acceso no autorizado.

**RF17 - Reportes personalizado de anomalías atendidas:** se realiza un reporte que guarda todas las anomalías que han sido atendidas.

**RF18–Activación de alarmas por áreas:** se activan las alarmas en cada una de las áreas de la entidad para controlar los accesos no autorizados y el movimiento de los activos en cada una de las mismas.

**RF19 –Anomalías registradas:** se procede a atender las anomalías que han sido registradas una vez activadas las alarmas.

### 2.4.2 Requisitos no funcionales

Una vez determinado lo que el sistema debe hacer se especifica el comportamiento que debe tener el mismo así como las cualidades que presentará. Los requisitos no funcionales responden a las características principales que debe cumplir el sistema para satisfacer el contrato.

Los requerimientos no funcionales son restricciones de los servicios o funciones ofrecidas por el sistema, incluyen restricciones de tiempo, sobre el proceso de desarrollo y estándares. A menudo son aplicados al sistema en su totalidad, escasamente se aplican a características o servicios individuales del sistema (40).

#### ✓ Usabilidad

## **CAPÍTULO 2. DISEÑO DEL SISTEMA PARA EL CONTROL DE ACCESO Y ACTIVOS FIJOS**

---

### **RNF1.1: Fácil interacción**

El sistema debe brindar una facilidad de uso que permita la fácil interacción con el mismo y llegar de manera rápida y efectiva a la opción deseada. Debe poseer además una interfaz de manejo cómodo que posibilite a los usuarios sin experiencia una rápida adaptación.

### **RNF1.2: Emplear perfiles de usuario**

Se deben emplear perfiles de usuario para diferenciar las interfaces y opciones para los usuarios que accedan al sistema según los diferentes roles que estos tengan dentro del mismo.

### **RNF1.3: Resolución de la página**

La resolución de la página se adaptará la resolución de pantalla en el cliente.

### ✓ **Confiabilidad**

#### **RNF2.1: Políticas de respaldo**

Se garantizarán políticas de respaldo a toda la información, evitando pérdidas en caso de desastres ajenos al sistema.

#### **RNF2.2: Eliminación de la información**

Ninguna información que se haya ingresado en el sistema será eliminada físicamente de la Base de Datos (BD), independientemente de que para el sistema, este elemento ya no exista.

### ✓ **Eficiencia**

#### **RNF3.1: Buenas prácticas de programación**

El sistema adoptará buenas prácticas de programación para incrementar el rendimiento en operaciones costosas para la máquina virtual como la creación de objetos.

### ✓ **Soporte**

#### **RNF4.1: Soporte y mantenimiento del sistema**

La Universidad de las Ciencias Informáticas debe garantizar el soporte y mantenimiento del sistema.

#### **RNF4.2: Documentación necesaria**

Debe existir toda la documentación necesaria que de apoyo a los especialistas en caso de que sea necesario hacer un mantenimiento inmediato al producto.

### ✓ **Restricciones de diseño**

#### **RNF5.1: Codificación**

La codificación se realizará siguiendo el estándar definido en el sistema.

#### **RNF5.2: Interfaces**

Las interfaces se realizarán siguiendo el estándar definido en el sistema.

### **RNF5.3: Nomenclatura**

La nomenclatura de las bases de datos, tablas, campos de las tablas, esquemas, procedimientos almacenados o funciones, vistas, triggers y tipos de datos se elaborarán siguiendo los estándares definidos en el centro.

#### ✓ **Interfaz**

### **RNF6.1: Interfaz de usuario**

Interfaz sencilla con colores suaves a la vista y sin cúmulo de imágenes u objetos que distraigan al cliente del objetivo.

### **RNF6.2: Coherencia y estilo**

Mantener una coherencia y estilo común entre todas las páginas.

### **RNF6.3: Interfaz de software**

En la base de datos es necesario que esté instalada una versión de PostgreSQL 8.4 o superior. Tecnologías necesarias: Máquina Virtual de Java (JVM, por sus siglas en inglés), *Java Runtime Environment* (JRE, por sus siglas en inglés).

#### ✓ **Estándares aplicables**

### **RNF7.1: Pautas de análisis**

Para las descripciones de casos de uso, mensajes y avisos que debe emitir el sistema, se deben seguir las pautas de análisis definidas en el centro.

### **RNF7.2: Codificación y diseño**

Para la implementación del sistema se deberá seguir los estándares de codificación y diseño definidos por el centro, fundamentalmente en el caso de los mensajes emitidos por la aplicación.

#### ✓ **Seguridad**

### **RNF8.1: Acceso de los usuarios**

Cada usuario realizará operaciones en la aplicación en dependencia de sus privilegios o niveles de acceso.

### **RNF8.2: Mensajes de verificación**

Ofrecer mensajes de verificación antes de ejecutar acciones irreversibles como pueden ser eliminación de datos.

#### ✓ **Portabilidad**

### **RNF9.1: Características del sistema**

El sistema debe ser multiplataforma, utilizado bajo los sistemas operativos Windows y cualquier distribución de Unix.

✓ **Rendimiento**

**RNF10.1: Procesamiento de datos y tiempo de respuesta**

Se debe contar con un rápido procesamiento de los datos y con un tiempo de respuesta mínimo.

### 2.5 Modelo del análisis

El modelo de análisis es la primera representación técnica de un sistema. Utiliza una mezcla de formatos en texto y diagramas para representar los requisitos del software, las funciones y el comportamiento. Debe cumplir tres objetivos primarios fundamentales: describir los que requiere el cliente, establecer una base para la creación de un diseño de software y definir un conjunto de requisitos que pueda validarse una vez construido el software. El mismo se complementa de cuatro elementos fundamentales. Estos elementos sirven para clasificar principalmente los diferentes diagramas, especificados en elementos de escenario, elementos de flujo, elementos de clases y elementos de comportamiento (41).

Hace mucho más fácil de comprender la representación propuesta inicialmente, ya que es posible examinar los requisitos desde diferentes puntos de vista, aumentando la probabilidad de encontrar errores, de que surjan debilidades y que se descubran descuidos. Ofrece al desarrollador y al cliente los medios para evaluar la calidad una vez construido el software.

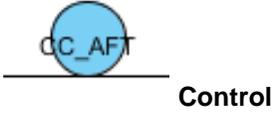
#### 2.5.1 Clases del análisis

El modelo de clases del análisis está centrado en los requisitos funcionales, su comportamiento está definido mediante responsabilidades definiendo atributos que son conceptuales y reconocibles en el dominio del problema. Participa en relaciones y encaja en uno de estos tres estereotipos básicos:

**Tabla 2.2. Descripción de las clases del análisis**

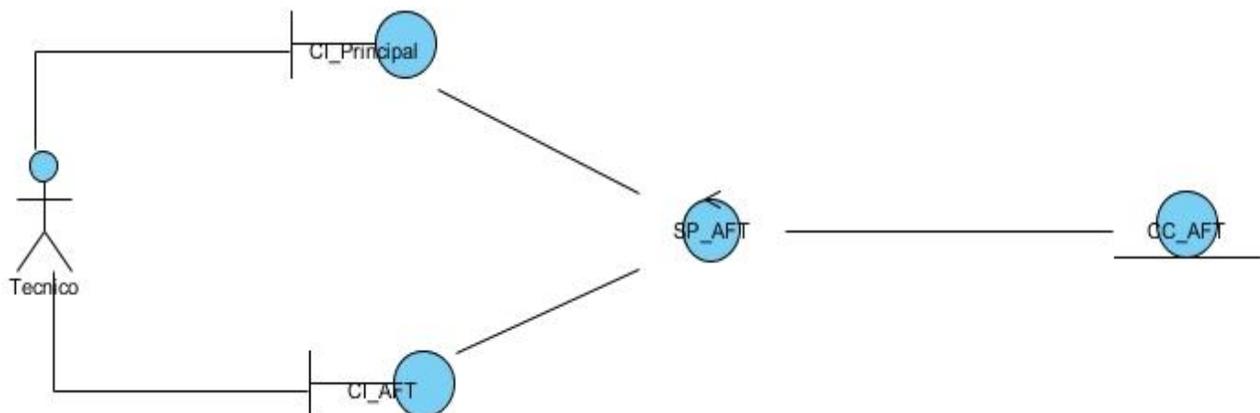
Nombre	Propósito
 <b>Entidad</b>	Modela la información que posee una vida larga y que a menudo es persistente, modelando la información y comportamiento asociado de algún fenómeno o concepto. Se derivan de una clase de entidad del negocio o del dominio.
 <b>Interfaz</b>	Modifica la interacción entre el sistema y sus actores, lo que implica recibir y representar informaciones y peticiones de los usuarios y sistemas externos. Representa la abstracción de ventanas, formularios, paneles, interfaz de comunicación, interfaz de impresión,

## CAPÍTULO 2. DISEÑO DEL SISTEMA PARA EL CONTROL DE ACCESO Y ACTIVOS FIJOS

	sensores, terminales, APIs, entre otros.
	Representa una coordinación secuencial, transacciones y control de otros objetos. Se usa para encapsular el control de un caso de uso en concreto y para representar derivaciones y cálculos complejos.

A continuación se muestran los diagramas de clases del análisis de mayor importancia, se recomienda ver el fichero del modelo de proceso de negocio que se encuentra en el expediente de proyecto para un mayor entendimiento.

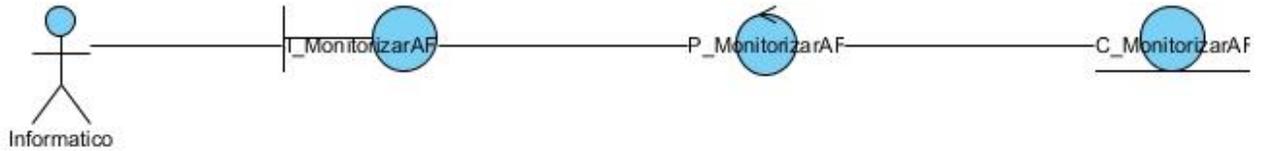
La figura 2.5 muestra el diagrama de clases del análisis de los activos fijos tangibles en la entidad, representa la relación existente entre el actor en este caso el técnico con las actividades pertenecientes en el mundo real.



**Figura 2.5. DCA adicionar AFT**

**Fuente: Elaboración propia**

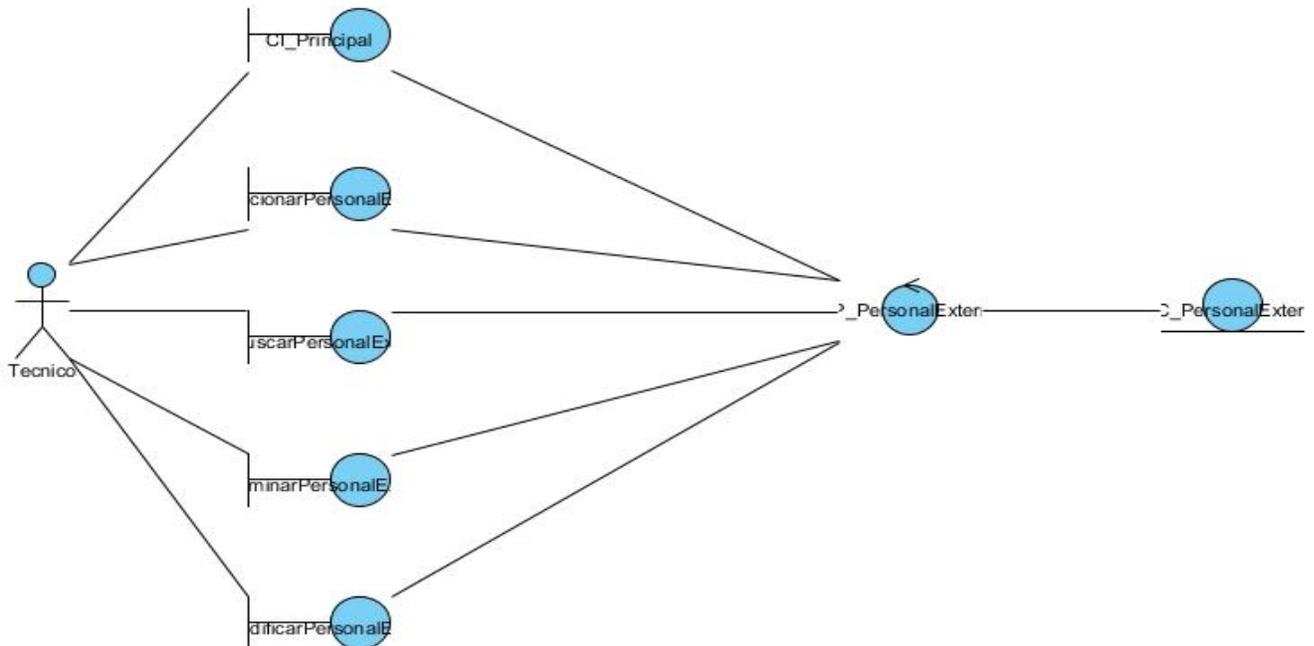
La figura 2.6 muestra el diagrama de clases del análisis del personal externo a la entidad, representando la relación existente entre el actor en este caso el informático con las actividades pertenecientes en el mundo real.



**Figura 2.6. DCA adicionar personal externo a la entidad**

**Fuente: Elaboración propia**

La figura 2.7 muestra el diagrama de clases del análisis de la monitorización de los activos fijos tangibles por las diferentes áreas de la entidad, representa la relación existente entre el actor en este caso el técnico con las actividades pertenecientes en el mundo real.



**Figura 2.7. DCA monitorizar AFT por área**

**Fuente: Elaboración propia**

La figura 2.8 muestra el diagrama de clases del análisis de la monitorización del acceso a las diferentes áreas de la entidad, representa la relación existente entre el actor en este caso el informático con las actividades pertenecientes en el mundo real.



Figura 2.8. DCA monitorizar acceso por área

Fuente: Elaboración propia

## 2.6 Modelo del diseño

En el modelo de diseño se estructura el sistema para que soporte tanto los requisitos funcionales como los no funcionales y las restricciones que se imponen, produciéndose un refinamiento del análisis y constituyéndose una base para la implementación. Durante la concepción del modelo de diseño son tenidos en cuenta un conjunto de patrones de diseño que influyen en la calidad del software a desarrollar.

### 2.6.1 Patrones de diseño

Los patrones de diseño son la base para la búsqueda de soluciones a problemas comunes en el desarrollo de software y otros ámbitos referentes al diseño de interacción o interfaces.

Un patrón de diseño es un modelo que se puede seguir para la realización de una actividad determinada, es una solución a un problema de diseño. Para que una solución sea considerada un patrón debe poseer ciertas características.

La figura 2.9 muestra una imagen del patrón arquitectónico Modelo Vista Controlador evidenciado en el componente propuesto para dar solución al problema a resolver.

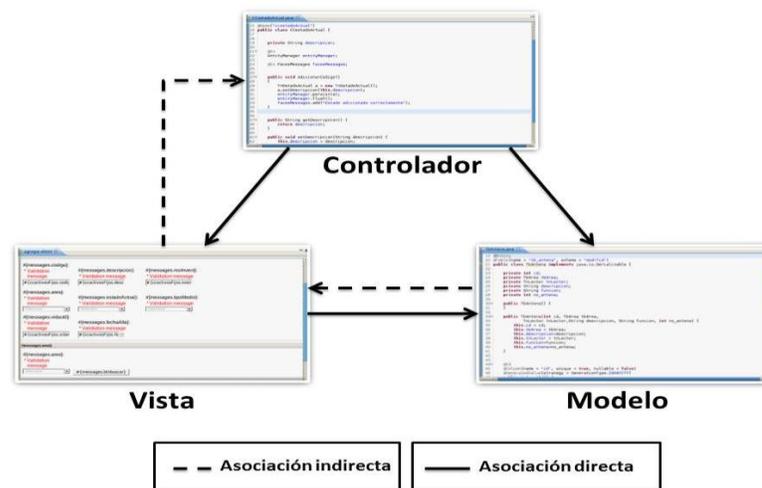


Figura 2.9. Patrón Arquitectónico Modelo Vista Controlador

Fuente: Elaboración propia

**Modelo Vista Controlador (MVC):** es un patrón de arquitectura de software que separa los datos de una aplicación, la interfaz de usuario, y la lógica de control en tres componentes distintos. El patrón MVC se ve frecuentemente en aplicaciones web, donde la vista es la página HTML y el código que provee de datos dinámicos a la página, el modelo es el Sistema de Gestión de Base de Datos y la Lógica de negocio, y el controlador es el responsable de recibir los eventos de entrada desde la vista. Utilizando este tipo de patrón es posible conseguir más calidad y un mantenimiento más fácil. Al margen de todo esto, una de las cosas más importantes que permite el uso de este patrón consiste en normalizar y estandarizar el desarrollo de Software. (42)

Las tres entidades que define este patrón son las siguientes:

- ✓ **Modelo:** administra el comportamiento y los datos del dominio de aplicación, responde a requerimientos de información sobre su estado y responde a instrucciones de cambiar el estado.
- ✓ **Vista:** la vista es el objeto que maneja la presentación visual de los datos gestionados por el Modelo. Este presenta el modelo en un formato adecuado para interactuar, usualmente la interfaz de usuario.
- ✓ **Controlador:** interpreta las acciones del usuario sobre el sistema, informando al modelo y/o a la vista para que cambien según resulte apropiado.

Los patrones utilizados en el desarrollo del sistema son los denominados Patrones Generales de Software para Asignación de Responsabilidades (GRASP) estos describen los principios fundamentales de diseño de objetos para la asignación de responsabilidades. Constituyen un apoyo para la enseñanza que ayuda a entender el diseño de objeto esencial y aplica el razonamiento para el diseño de una forma sistemática, racional y explicable.

Entre estos patrones destacan por su utilización:

- **Experto:** es un patrón que se usa más que cualquier otro al asignar responsabilidades; es un principio básico que suele utilizarse en el diseño orientado a objetos. Expresa simplemente la “intuición” de que los objetos hacen cosas relacionadas con la información que poseen. Se conserva el encapsulamiento, ya que los objetos se valen de su propia información para hacer lo que se les pide. Esto soporta un bajo acoplamiento, lo que favorece el hecho de tener sistemas más robustos y de fácil mantenimiento.

La figura 2.10 muestra una imagen del patrón de diseño Experto utilizado en el componente y su evidencia en el mismo.

### Patrón Experto:



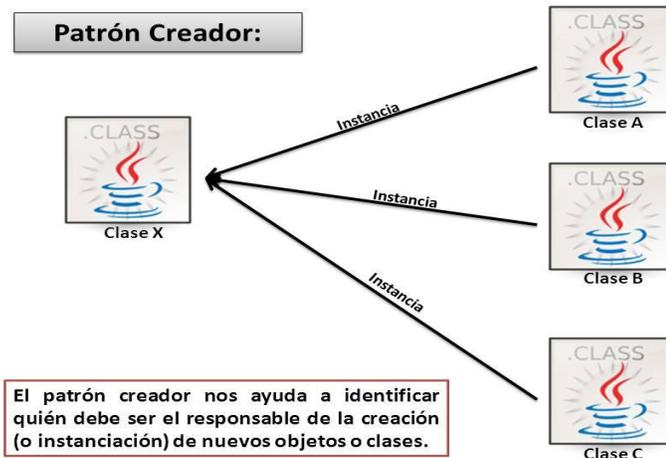
El patrón experto especifica que toda la responsabilidad recae sobre la clase que conoce toda la información necesaria para crearlo, así la información se mantiene encapsulada.

Figura 2.10. Patrón de diseño Experto

Fuente: Elaboración propia

- **Creador:** este patrón ayuda a identificar quién debe ser el responsable de la creación de nuevos objetos o clases. La nueva instancia deberá ser creada por la clase que tiene la información necesaria para realizar la creación del objeto, usa directamente las instancias creadas del objeto, almacena o maneja varias instancias de la clase.

La figura 2.11 muestra una imagen del patrón de diseño Creador utilizado en el componente y su evidencia en el mismo.



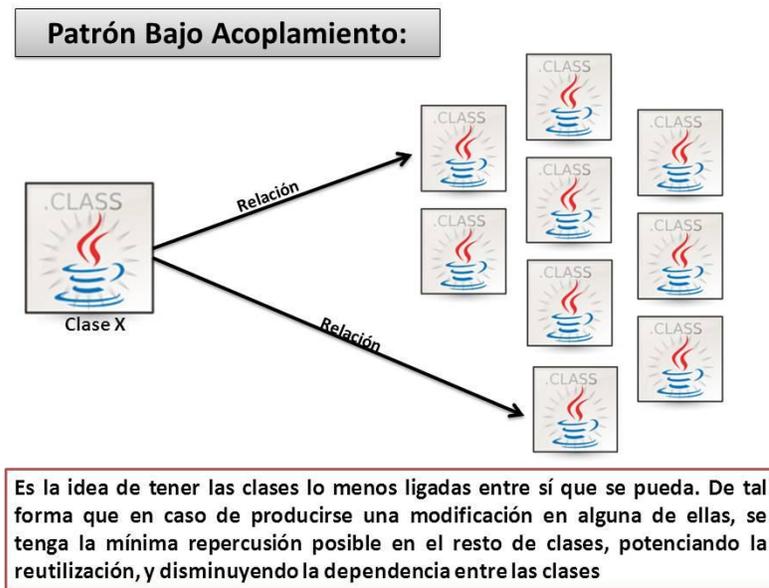
El patrón creador nos ayuda a identificar quién debe ser el responsable de la creación (o instanciación) de nuevos objetos o clases.

Figura 2.11. Patrón de diseño Creador

Fuente: Elaboración propia

- **Alta Cohesión:** es la medida de la fuerza que une a las responsabilidades de una clase. Una clase con baja cohesión es aquella que hace muchas cosas no afines o muchas tareas, lo que trae como consecuencias dificultades para entender, reutilizar y conservarla. Son delicadas y las afectan constantemente los cambios. Una clase con alta cohesión mejora la claridad y la facilidad de su uso, su mantenimiento se simplifica y es fácil de reutilizar. A menudo se genera un bajo acoplamiento.
- **Bajo acoplamiento:** es la medida de la fuerza con que una clase está conectada a otras clases. De tal forma que en caso de producirse una modificación en alguna de ellas, se tenga la mínima repercusión posible en el resto de clases, potenciando la reutilización, y disminuyendo la dependencia entre las clases.

La figura 2.12 muestra una imagen del patrón de diseño Bajo Acoplamiento utilizado en el componente y su evidencia en el mismo.



**Figura 2.12. Patrón de diseño Bajo Acoplamiento**

**Fuente: Elaboración propia**

- **Controlador:** Consiste en asignar una responsabilidad de recibir o manejar un mensaje de evento del sistema a una clase (43).

Estos patrones se aplicaron en la definición de cada clase del sistema con el objetivo de lograr que las clases cumplan las funciones específicas de cada una sin que se sobrecarguen (experto).

Las relaciones entre clases están limitadas solamente a la dependencia de conceptos, por lo que cada clase solamente se relaciona con aquellas cuyos conceptos dependen completamente de ella asegurando la mínima comunicación posible (bajo acoplamiento). Se definieron las clases controladoras de forma que cada una solo realiza un conjunto de tareas específicas sin suplantar las responsabilidades de otra (alta cohesión). Se le dio la responsabilidad de instanciar a una clase a aquellas clases que contengan a la misma (creador).

### 2.7 Diagramas de clases del diseño

Los diagramas de clases del diseño, son diagramas de estructura estática que se encargan de describir el comportamiento del sistema, mostrando las clases, los atributos y las relaciones entre ellos.

Una vez conocidos los casos de usos presentes en el sistema y conformados los diagramas de clases del análisis, se muestran a continuación los diagramas de clases del diseño más importantes.

La figura 2.13 muestra el diagrama de clases del diseño de los activos fijos tangibles. Describe el comportamiento que presentan los mismos desde su arribo a la entidad, así como la relación entre las clases y atributos.

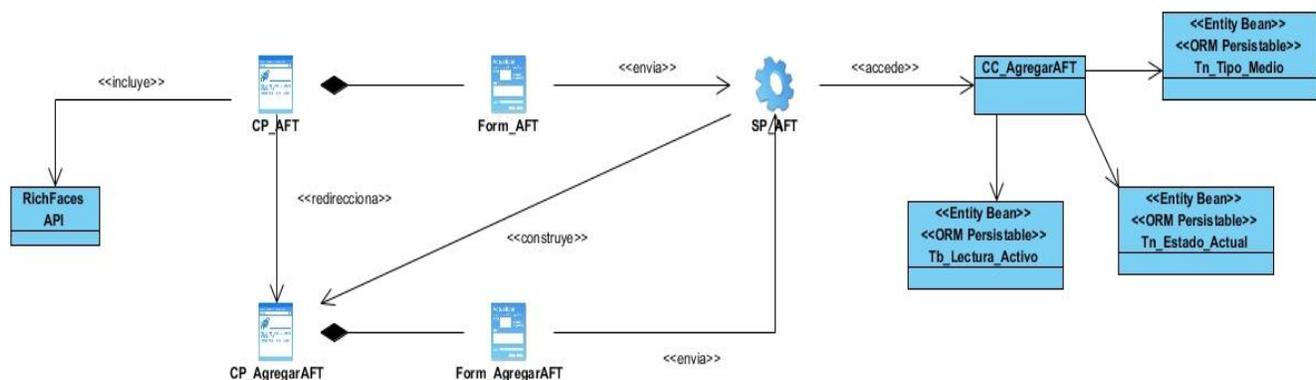


Figura 2.13. DCD adicionar AFT

Fuente: Elaboración propia

## CAPÍTULO 2. DISEÑO DEL SISTEMA PARA EL CONTROL DE ACCESO Y ACTIVOS FIJOS

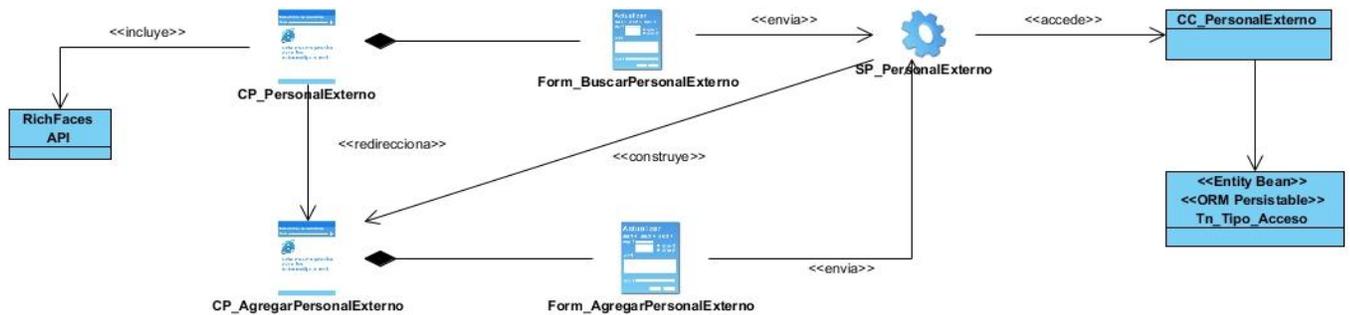


Figura 2.14. DCD adicionar personal externo a la entidad

Fuente: Elaboración propia

La figura 2.15 muestra el diagrama de clases del diseño de la monitorización de los activos fijos tangibles por áreas de la entidad. Describe el comportamiento, la relación entre las clases y los atributos.

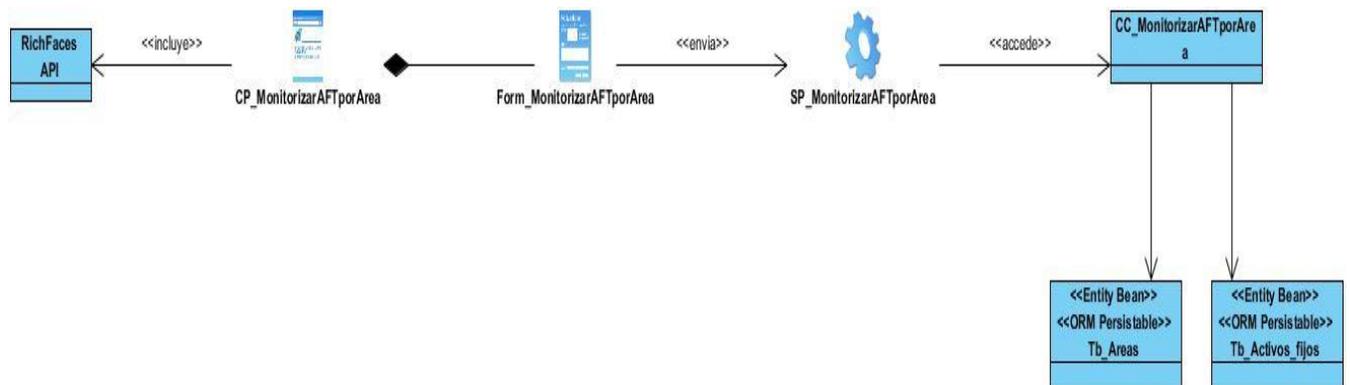


Figura 2.15. DCD monitorizar AFT por área

Fuente: Elaboración propia

La figura 2.16 muestra el diagrama de clases del diseño monitorizar acceso por área. Describe el comportamiento que presenta desde que un personal accede a las diferentes áreas de la entidad, así como la relación entre las clases y atributos.

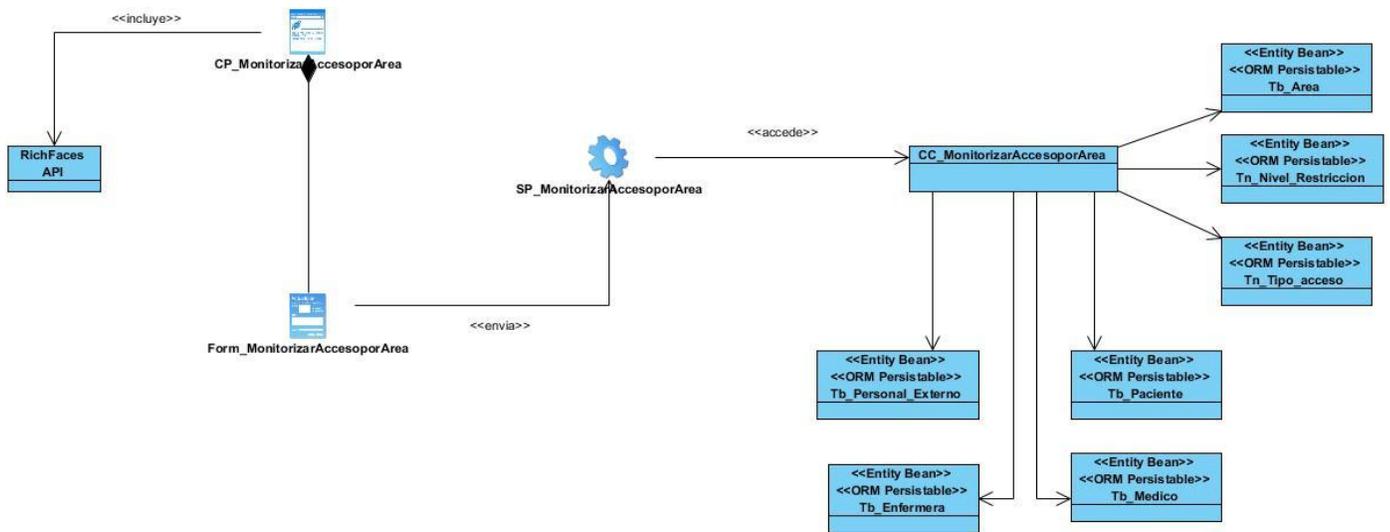


Figura 2.16. DCD monitorizar acceso por área

Fuente: Elaboración propia

### 2.7.1 Descripción de las clases del diseño

La representación de las clases del diseño está asociada al uso de UML para el modelado de aplicaciones WEB, siendo identificadas las siguientes clases: página servidora (*server page*), página cliente (*client page*), formulario (*form*).

Tabla 2.3. Descripción de las clases del diseño

Nombre	Propósito
 <b>(Client Page)</b>	Proveer la interacción con el usuario, permiten al usuario realizar las peticiones e interactuar con la aplicación.
 <b>(Form)</b>	Las clases formularios representan la entrada y salida de datos en el sistema. Estos datos son primeramente validados y luego enviados a la clase controladora correspondiente.
 <b>(Server Page)</b>	Son las encargadas de procesar las peticiones de los usuarios y de realizar los cambios apropiados en el modelo o en la vista.

### 2.7.2 Diagrama de interacción

Un diagrama de interacción, representa la forma en como un cliente (actor) u objetos (clases) se comunican entre sí en petición a un evento. Esto implica recorrer toda la secuencia de llamadas, de donde

## **CAPÍTULO 2. DISEÑO DEL SISTEMA PARA EL CONTROL DE ACCESO Y ACTIVOS FIJOS**

---

se obtienen las responsabilidades claramente. Este diagrama puede ser de dos tipos: de secuencia y de colaboración.

Se realizaron los diagramas de comunicación para dar cumplimiento al diseño de la aplicación, el mismo muestra la interacción de un conjunto de objetos que envían y reciben mensajes, se recomienda ver en el fichero del modelo de proceso de negocio que se encuentra en el expediente de proyecto para un mayor entendimiento.

### **2.8 Modelo de datos.**

El modelo de datos describe de forma abstracta las entidades y sus características, además de las relaciones entre estas dentro de la base de datos. Este lenguaje permite detallar los elementos de un problema y la forma en que se relacionan en la vida real.

A continuación la figura 2.17 muestra el modelo de datos establecido que contiene de forma detallada y clara los tipos de datos, relaciones y restricciones que lo componen.

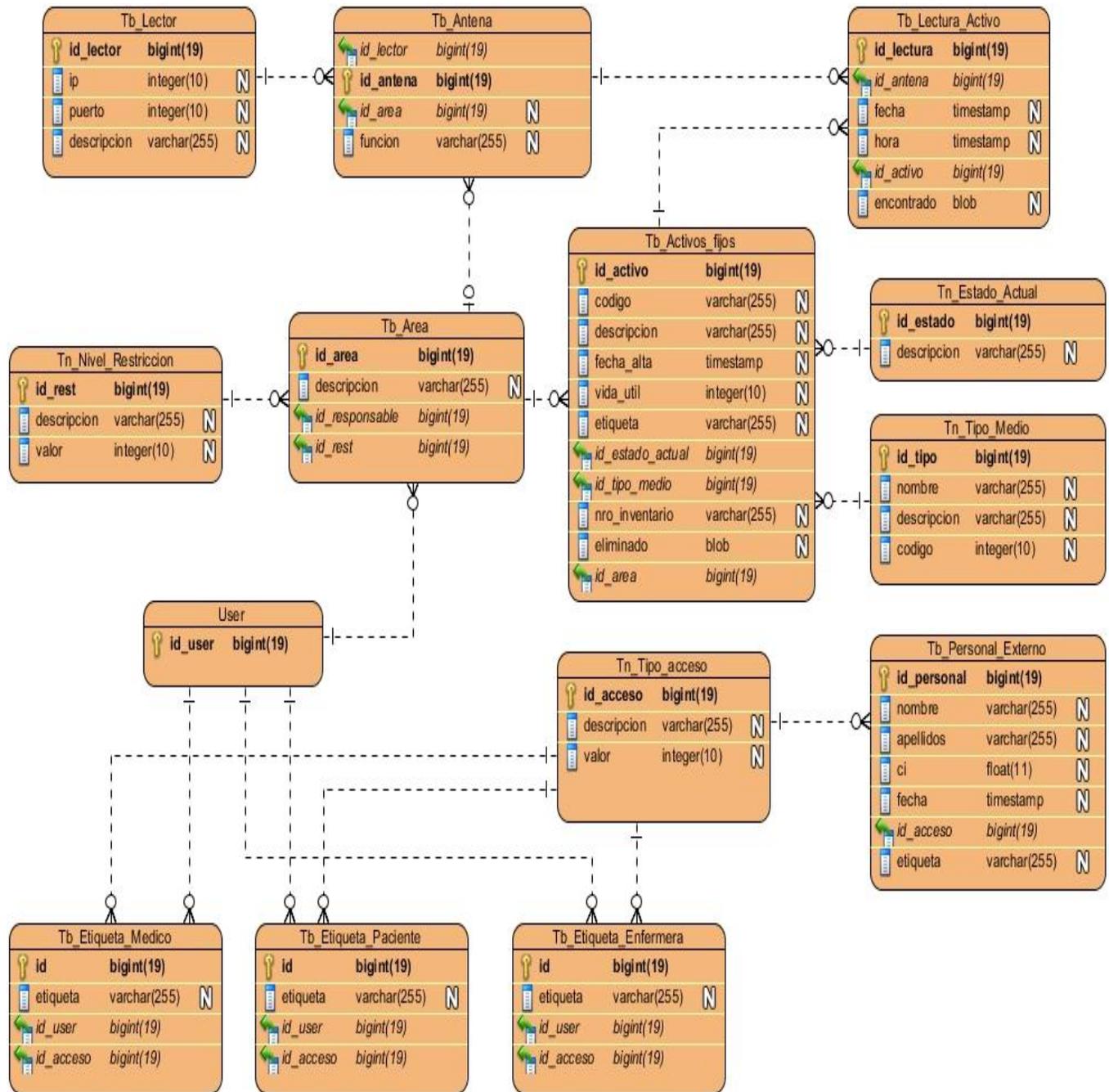


Figura 2.17. Modelo de datos

Fuente: elaboración propia

### 2.9 Selección de equipos y análisis de costo

Para la selección de los equipos RFID propuestos se establecieron parámetros en la tecnología como frecuencia de operación, tipos de etiquetas y lectores a utilizar. Se realizó un estudio sobre el rango de lectura necesario al que se espera identificar las etiquetas, el cual debe estar en un máximo de 10mts de distancia entre las antenas y las etiquetas. La frecuencia de operación debe ser de campo cercano, recomendando la ultra alta frecuencia (UHF, por sus siglas en inglés) entre los rangos de 860 MHz a 960 MHz, esta frecuencia es muy difundida y utilizada en las aplicaciones de trazabilidad de productos y acceso a edificios.

Entre los equipos propuestos a usar se encuentran:

- Etiqueta Gen2 UHF

**Tabla 2.4. Etiqueta UHF**

<b>Frecuencia de operación</b>	860 MHz a 960 MHz
<b>Protocolos</b>	EPC Class 1 Gen2, ISO 18000-6C
<b>Tamaño</b>	97 mm x 15 mm
<b>Rango de lectura</b>	Hasta 12m
<b>Resistente</b>	Agua/Polvo

Es ampliamente utilizada para aplicaciones de la cadena de suministro, seguimiento de envases reutilizables, gestión y control de inventarios y de seguimiento de activos en general.

- Lector Gen2 de largo alcance

**Tabla 2.5. Lector Gen2 de largo alcance**

<b>Frecuencia de operación</b>	860 MHz a 960 MHz
<b>Protocolos</b>	EPC Class1 Gen1 y Gen2
<b>Compatibilidad antenas</b>	Hasta 12 dBi
<b>Rango Lectura/Escritura</b>	Hasta 15m
<b>Tamaño</b>	460 x 460 x 50 mm

## CAPÍTULO 2. DISEÑO DEL SISTEMA PARA EL CONTROL DE ACCESO Y ACTIVOS FIJOS

Este lector ha sido diseñado para entornos industriales. Es compatible con EPC Class1 Gen1 y Gen2 y opera en la banda de UHF de 860-960 MHz. El largo alcance del lector funciona bien incluso en entornos difíciles.

- Lector USB RFID UHF de escritorio

**Tabla 2.6. Lector USB RFID UHF de escritorio**

<b>Frecuencia de operación</b>	860 MHz a 960 MHz
<b>Protocolos</b>	ISO18000-6B, ISO18000-6C(EPC C1G2)
<b>Compatibilidad antenas</b>	Hasta 10 dBi
<b>Rango Lectura/Escritura</b>	Hasta 200 mm
<b>Tamaño</b>	15 x 10 x 6.0 cm

EL lector USB RFID UHF de escritorio está diseñado para el etiquetado de paquetes o inventarios. Soporta la interfaz de USB 1.1, además no necesita una fuente de energía externa.

- Antena Alien Circular

**Tabla 2.7. Antena Alien Circular**

<b>Frecuencia de operación</b>	890 MHz a 940 MHz
<b>Polarización</b>	Circular
<b>Ganancia</b>	7 dBi
<b>Tamaño</b>	240*240*30mm

Utiliza la más alta tecnología de polarización circular que distribuye la energía de UHF uniformemente en una pauta radialmente simétrica, proporcionando la habilidad de leer las etiquetas a pesar de la orientación en que se encuentre.

En la siguiente tabla se pueden apreciar los diferentes precios que poseen los equipos seleccionados. Vale acotarse que el precio de estos equipos en el mercado internacional es en dólares.

**Tabla 2.8. Precios de equipos RFID**

<b>Equipos RFID</b>	<i>Etiqueta 115004 UHF</i>	<i>Lector 216010 Gen2</i>	<i>Antena Alien</i>	<i>Lector USB</i>
<b>Precios</b>	\$0.66	\$980	\$295	\$252

## **CAPÍTULO 2. DISEÑO DEL SISTEMA PARA EL CONTROL DE ACCESO Y ACTIVOS FIJOS**

---

En este capítulo se plasma una propuesta de solución para lograr el desarrollo de la aplicación, además se hace un estudio detallado de los requisitos de software donde a partir de los requisitos funcionales se crean todas las funcionalidades que detallará el sistema. Se obtuvo el modelo de diseño, identificándose y describiéndose las clases necesarias para el correcto funcionamiento del sistema. Se definieron los patrones a utilizar como son: GRASP y MVC, se incorporaron los beneficios desde el punto de vista arquitectónico y tecnológico que proveen. Además se confeccionaron los diagramas de clases del diseño proporcionándole al desarrollador una idea más clara de lo que debe implementar.

## **Capítulo 3: Implementación del sistema para el control de acceso y activos fijos**

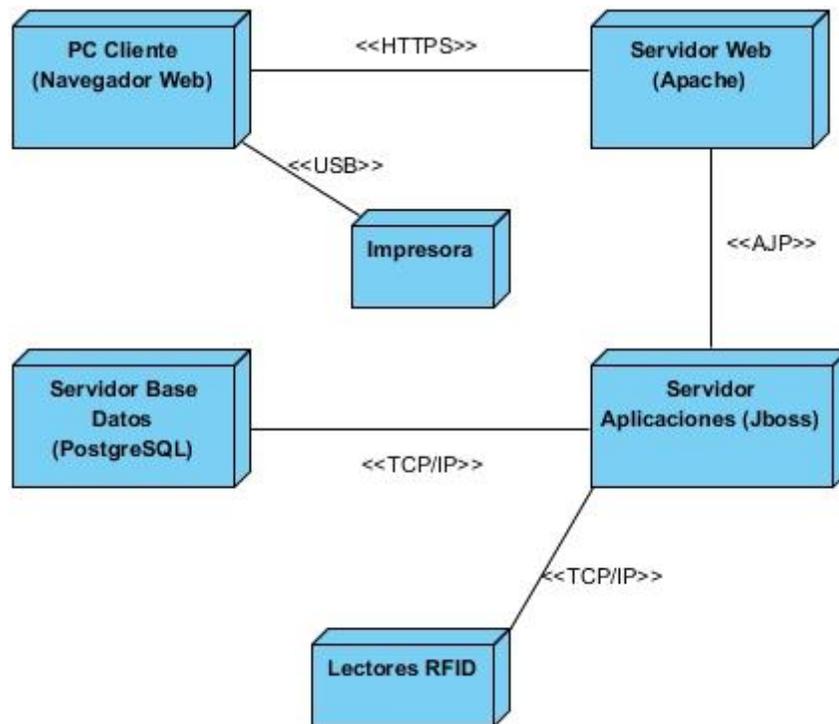
Este capítulo constituye la continuidad del modelo de diseño, implementando en términos de componentes las clases y subsistemas obtenidos en la disciplina anterior, posee como propósito fundamental aplicar la arquitectura concebida y descrita anteriormente para sustentar el desarrollo del sistema. Además se realiza un estudio de los estándares de codificación, estilos y tratamientos de errores a utilizar en la implementación del sistema.

### **3.1 Integración con otros sistemas.**

Con el objetivo de reutilizar software existente y por tanto disminuir los costos, en la actualidad no se concibe ningún sistema de forma aislada por lo que se hace necesario pensar en su integración con otros sistemas en funcionamiento o en vías de desarrollo. La aplicación del componente RFID no es la excepción. El mismo forma parte del sistema xavia HIS y mantiene una estrecha relación con los restantes módulos del sistema. El módulo de configuración brinda información útil y necesaria al módulo Monitorización y éste a su vez brinda servicios los cuales son utilizados por este sistema.

### **3.2 Diagrama de despliegue**

El Diagrama de Despliegue es el tipo de diagrama del UML, que se utiliza para modelar el hardware utilizado en las implementaciones de sistemas y las relaciones entre sus componentes. Los elementos usados por este tipo de diagrama son los nodos, componentes y asociaciones. Su objetivo es mostrar cómo y dónde se desplegará el sistema. Los mismos muestran las relaciones físicas de los distintos nodos que componen un sistema y el reparto de los componentes sobre dichos nodos. El diagrama de despliegue de la solución propuesta se ilustra en la figura 3.1 mostrada a continuación:



**Figura 3.1. Diagrama de despliegue**  
 Fuente: elaboración propia

### Descripción de los elementos

**Estaciones Clientes (Navegador Web):** serán las estaciones de los usuarios, las cuales servirán para acceder al sistema web o integrado mediante el navegador.

**Servidor Web (Apache):** servidor Web Apache que provee el servicio de interfaz al usuario final mediante un portal convencional, pues es el ordenador que estará como fachada a Internet, al mismo tiempo será el puente o proxy para entrar al clúster de servidor de aplicaciones que proporciona Jboss.

**Servidor de Aplicaciones (Jboss):** Servidor de Aplicaciones Jboss certificado por SUN para el estándar JEE5, hospedará la solución integrada, proveerá de un clúster para balancear la carga de peticiones hechas por los usuarios garantizando de esta manera disponibilidad de la información mostrada.

**Servidor de Bases de Datos (PostgreSQL):** Servidor de Datos PostgreSQL, en el cual residirá toda la información operacional.

**Lector RFID:** dispositivo encargado de crear el campo de radiofrecuencia y capturar la información de las etiquetas. Envía cada en cada momento la información hacia el servidor de aplicaciones.

**Dispositivo Impresora:** dispositivo conectado a las estaciones clientes de los usuarios que permitirá realizar la impresión de los reportes del sistema.

**Procesadores:**

**Servidor(es) de Aplicaciones:**

Sistema Operativo Linux  
2 DL380 G5,  
Procesador Intel® Xeon® 5140 Dual - Core  
4GB de memoria  
2x72GB de disco

**Servidor de Base de Datos:**

Sistema Operativo Linux  
1 DL380 G5  
Procesador Intel® Xeon® 5140 Dual – Core  
4GB de memoria

**Servidor Web:**

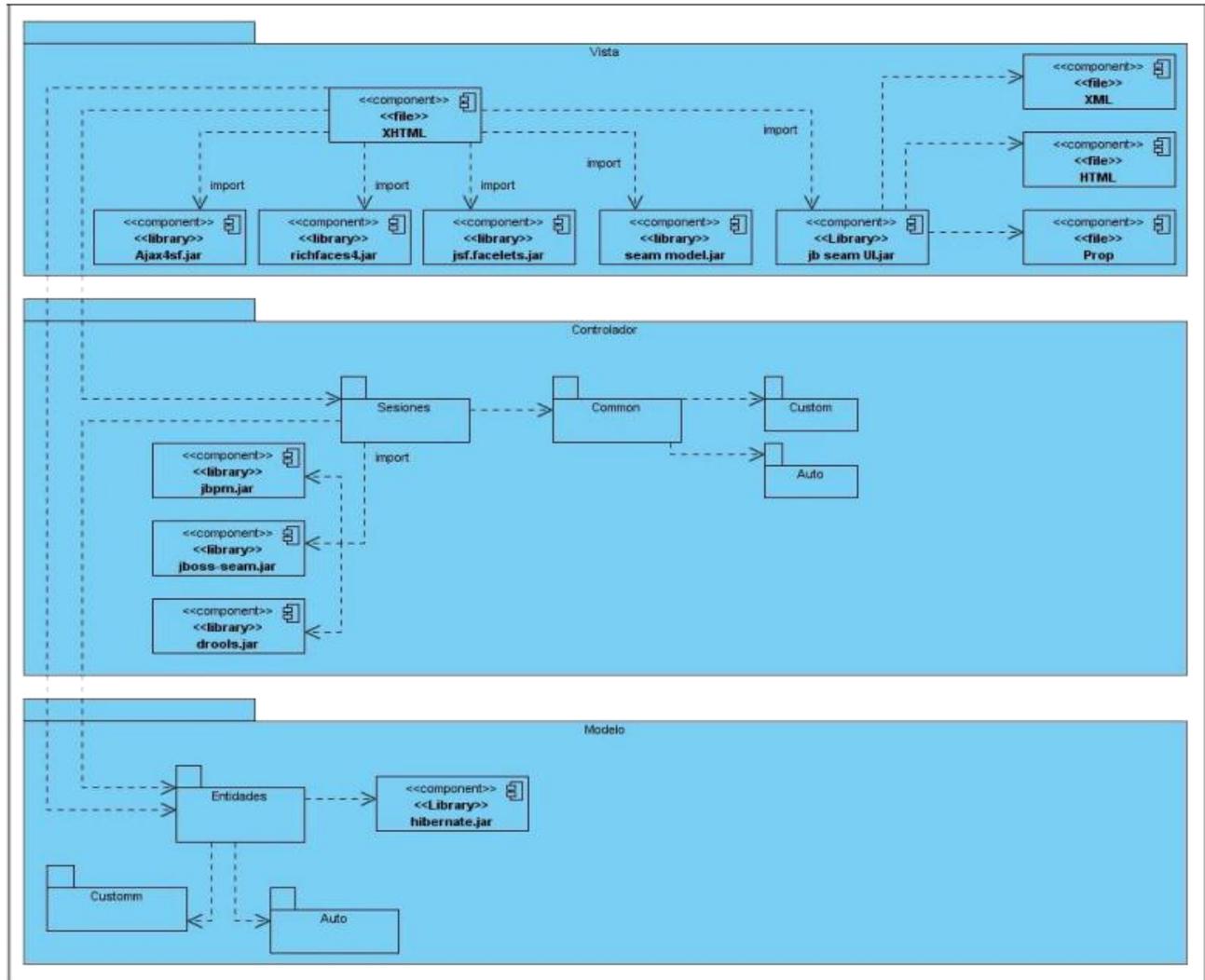
Sistema Operativo Linux  
1 DL380 G5  
Procesador Intel® Xeon® 5140 Dual - Core  
2 GB de memoria  
2x72GB de disco

**Estaciones Clientes:**

Sistema Operativo Linux.  
IE 7, Firefox 6.0 o versiones superiores.  
256 Mb de memoria RAM  
Microprocesador de 2.0 Hz

### **3.3 Diagrama de componentes**

Los diagramas de componentes muestran los componentes de software (ficheros de código fuente, scripts, ficheros de código binario, ejecutables y similares) y las relaciones que existen entre ellos. Cada componente puede agruparse en paquetes para obtener una mejor organización y simplificar la implementación.



**Figura 3.2. Diagrama de componentes**  
 Fuente: elaboración propia

### 3.4 Tratamiento de excepciones

Las excepciones son definidas como errores que interrumpen el flujo normal de las sentencias de un programa. Realizar el tratamiento de estas excepciones le brinda robustez y flexibilidad al sistema, ya que permite que el programa siga ejecutándose a un teniendo un error, cuando dicho error ocurre dentro de un método Java, automáticamente se crea un objeto “*Excepción*” el cual es tratado en el sistema de

ejecución. Este objeto contiene información sobre la excepción, incluyendo su tipo y el estado del programa cuando ocurrió el error. El tratamiento de estos errores se realiza usando la siguiente sentencia:

```
try  
{  
//declaración de código que causa la excepción  
}  
catch( Nombre de Excepción obj)  
{  
//código para tratar el error  
}
```

En el sistema propuesto se utilizan todas las facilidades que brinda la plataforma para el tratamiento de excepciones. Para cada fragmento de código donde se espere una situación anómala, se definen las excepciones correspondientes para luego ser tratadas evitando la interrupción del sistema. La siguiente figura hace referencia a su uso en una de las clases del sistema desarrollado:

```
public void eliminarInstanciaEntidad()  
{  
    for(int i=0;i<motivosEliminar.size();i++)  
    {  
        try  
        {  
            entityManager.remove(motivosEliminar.get(i));  
            entityManager.flush();  
        }  
        catch (Exception e)  
        {  
            facesMessages.add("Error, valor asociados:"+motivosEliminar.get(i).getDescripcion());  
            facesMessages.addFromResourceBundle("mensaje_inf_asociada");  
            return;  
        }  
    }  
}
```

**Figura 3.3. Tratamiento de excepciones**  
**Fuente: elaboración propia**

En caso de ocurrir una excepción que implique una redirección, se maneja mediante los denominados `pages.xml`, los mismos se encargan de capturar globalmente las excepciones y ejecutar las

instrucciones determinadas. Junto a esto se utiliza el componente *Seam FacesMessages*, propio de *framework Seam*, que captura los mensajes de excepción provenientes de las clases controladoras, y permite mostrarlos en las interfaces de usuario.

### **3.5 Seguridad**

La seguridad es de gran importancia para cualquier sistema de información, para obtener un sistema seguro se debe garantizar la integridad, confidencialidad y disponibilidad de la información. La mezcla de estas características trae consigo que la información sea modificada y vista por el personal autorizado. A continuación se presentan un conjunto de acciones llevadas a cabo para contar con sistema seguro:

- El acceso al sistema estará regido por un módulo de autenticación, usuario-contraseña, el cual solo dará permiso a acceder a aquellos personas permitidas.
- Se realiza además el control a nivel de usuarios y contraseñas, garantizando el acceso sólo a los niveles establecidos de acuerdo con la función que realiza cada usuario. Estas reglas son creadas en el módulo Configuración, atendiendo a la función del usuario en el sistema. Esto puede llevarse a cabo por la posibilidad de integración con el motor de reglas JBoss Rules, que brinda el framework JBoss Seam.
- Las contraseñas tendrán un nivel de complejidad alto, fortaleciendo así al sistema ante posibles intromisiones o accesos indebidos.
- Se realiza una traza de todas las acciones efectuadas por cada usuario autenticado en el sistema, mediante el uso de una bitácora.
- Se deben realizar salvases periódicas de la información contenida en los sistemas gestores de datos para evitar las pérdidas de datos por algún suceso ajeno al sistema.

### **3.6 Principales funcionalidades**

Para tener una mejor comprensión sobre el componente desarrollado, se muestran a continuación las funcionalidades más importantes desarrolladas en el componente y sus resultados en tiempo real haciendo uso del simulador.

# CAPÍTULO 3. IMPLEMENTACIÓN DEL SISTEMA PARA EL CONTROL DE ACCESO Y ACTIVOS FIJOS

La figura 3.4 muestra la funcionalidad monitorización del personal por áreas, permite monitorizar en tiempo real el personal que accede a un área determinada, mostrando si posee acceso o no para estar en la misma.

Monitorización del personal por áreas Buscar...

**Criterios de búsqueda**

Área: Consulta Buscar Cancelar

**Información sobre el personal**

Personal con acceso pleno al área seleccionada

Personal sin acceso al área seleccionada

**Listado del personal**

<input type="checkbox"/>	Etiqueta	Nombre	Apellidos	Acceso	Ocupación	
<input type="checkbox"/>	35e7e7fb84c976738fed5e02	Julia	Pop LA	Nivel3	Externo	
<input type="checkbox"/>	350225124be0ba8022ae1efd	Administrador	Administrador	Nivel4	Medico	
<input type="checkbox"/>	35ba3739ffa4ed719707745b	Oliver Salvador	Santana	Nivel3	Enfermera	
<input type="checkbox"/>	351d38b6219d01565d874841	Ramon	Pérez	Nivel3	Paciente	

**Figura 3.4. Monitorización del personal por áreas**  
Fuente: elaboración propia

La funcionalidad monitorización de activos fijos tangibles por áreas, la cual se muestra en la figura 3.5, brinda la posibilidad de observar en tiempo real los activos de un área determinada, proporciona información detallada en caso de que el activo se encuentre, no se encuentre, o no pertenezca al área seleccionada.

Monitorización de activos fijos tangibles por áreas Buscar...

**Criterios de búsqueda**

Área: Consulta Buscar Cancelar

**Información sobre los activos fijos tangibles**

Activos no encontrados en el área seleccionada

Activos encontrados en el área seleccionada

Activos no asignados al área seleccionada

**Listado de activos fijos**

<input type="checkbox"/>	Código	Etiqueta	Descripcion	Nro Inv.	Vida útil	Área	Estado	Tipo de medio	Fecha	
<input type="checkbox"/>	05FE45	100205910e13a35cfa375aa5	mesa	000111	10	Finanzas	Oscioso	Muebles, enseres y equipos de oficina	2013-02-11	
<input type="checkbox"/>	05RTE5JN	1001076dd2c325426dd2e2d8	microscopio	02541455	8	Consulta	Activo	Muebles, enseres y equipos de oficina	2013-03-12	
<input type="checkbox"/>	071AS78	10030f7815994e086b7ba41f	camilla	010358	9	Consulta	Activo	Equipos no tecnológicos	2013-02-05	
<input type="checkbox"/>	071AS78	1002095f2961ce9a13bc5e5f	silla	000122	7	Consulta	Oscioso	Muebles, enseres y equipos de oficina	2013-02-05	

**Figura 3.5. Monitorización de activos fijos por áreas**  
Fuente: elaboración propia

La figura 3.6 hace referencia a la funcionalidad de activación de alarmas de control, las cuales una vez que sean activadas comprobaran en tiempo real el personal y los activos fijos del área donde ha sido activada para registrar todas las anomalías que ocurran.

The screenshot shows a web application window titled 'Sistema de activación de alarmas'. It features a search bar labeled 'Buscar...' in the top right corner. Below the title bar is a green header with the word 'Alarmas'. Underneath, there is a sub-header 'Áreas' followed by a table. The table has four columns: 'Descripcion', 'Responsable', 'Nivel de restricción', and an icon column. Each row represents an area with a checkbox, a description, a responsible person, a restriction level, and a status icon (either a red shield with a white 'X' or a green shield with a white checkmark).

<input type="checkbox"/>	Descripcion	Responsable	Nivel de restricción	
<input type="checkbox"/>	Recepcion	Carlos	Área Pública	
<input type="checkbox"/>	Direccion	María	Área Restringida	
<input type="checkbox"/>	Consulta	Roger	Área Estándar	
<input type="checkbox"/>	Salon Espera	Ana	Área Pública	
<input type="checkbox"/>	Finanzas	Tania	Área Segura	
<input type="checkbox"/>	Almacen	Héctor	Área Restringida	

**Figura 3.6. Sistema de activación de alarmas por áreas**  
Fuente: elaboración propia

La funcionalidad de notificaciones de anomalías registradas, ocurren en tiempo real a medida que están activadas las alarmas y estas van registrando sucesos sobre los activos y el personal, los cuales pueden ser desde violaciones a un área, hasta pérdidas de activos. La figura 3.7 muestra la interfaz de la funcionalidad.

Anomalías registradas Q Buscar...

**Anomalías**

Listado de anomalías pendientes de revisión

<input type="checkbox"/>	Nombre	Ocupación	Area	Fecha	
<input type="checkbox"/>	Ramon	Paciente	Consulta	2013-04-10 03:08:23.054	
<input type="checkbox"/>	Julián	Paciente	Finanzas	2013-04-10 03:11:44.515	
<input type="checkbox"/>	Julián	Paciente	Finanzas	2013-04-10 03:42:25.998	
<input type="checkbox"/>	Julián	Paciente	Finanzas	2013-04-10 03:13:30.378	
<input type="checkbox"/>	Julián	Paciente	Finanzas	2013-04-10 03:25:26.749	

**Figura 3.7. Notificaciones de anomalías registradas**  
 Fuente: elaboración propia

### 3.7 Estándar de codificación

Los estándares de codificación son un conjunto de reglas que guían a los desarrolladores para escribir un código fuente que sea entendible y posea una adecuada comprensión para que en un futuro se le pueda dar mantenimiento al sistema, posibilitando además una mayor organización y limpieza en el código.

A continuación se describen una serie de estrategias de codificación a utilizar para la implementación del sistema, definidas por el centro y aplicados en el xavia HIS:

- Se debe usar siempre una línea en blanco en las siguientes circunstancias:
  - Entre métodos.
  - Entre las variables locales de un método y su primera sentencia.
  - Antes de un comentario de bloque o de un comentario de una línea.
  - Entre las distintas secciones lógicas de un método para facilitar la lectura.
- Respecto a la indentación y longitud de la línea:

- Se deben emplear cuatro espacios como unidad de indentación. La construcción exacta de la indentación (espacios en blanco contra tabuladores) no se especifica. Los tabuladores deben ser exactamente cada 8 espacios.
- Evitar las líneas de más de 80 caracteres, ya que no son manejadas bien por muchas terminales y herramientas.
- Respecto a las normas de inicialización, declaración y colocación de variables, constantes, clases y métodos:
  - Los nombres de las variables deben ser cortos pero con significado.
  - Los nombres de variables de un solo carácter se deben evitar, excepto para variables índices temporales.
  - Los nombres de las clases deben ser sustantivos, cuando son compuestos tendrán la primera letra de cada palabra que lo forma en mayúscula. Mantener los nombres de las clases simples y descriptivas. Usar palabras completas, evitar acrónimos y abreviaturas.
  - Los métodos deben ser verbos, cuando son compuestos tendrán la primera letra en minúscula y la primera letra de las siguientes palabras que lo forman en mayúscula.

En este capítulo se describieron las tablas que conforman el modelo de datos del sistema presentado. Se construyeron los diagramas de componente y despliegue estrechamente relacionados con el modelo de diseño. Se especificó la estrategia de codificación para la implementación de las funcionalidades, así como los estándares y estilos a utilizar. De igual manera fue descrita la concepción del tratamiento de errores, así como la seguridad del sistema.

### Conclusiones

Con el desarrollo del componente para el control de acceso y activos fijos en el Sistema de Información Hospitalaria xavia HIS, utilizando la tecnología de Identificación por Radiofrecuencia, se tienen en cuenta las tareas trazadas para la investigación y se da solución al problema propuesto, por lo que se pueden arribar a las siguientes conclusiones:

- El estudio de la génesis y evolución de la tecnología de Identificación por Radiofrecuencia, brindó un punto de partida para la realización del componente propuesto.
- El análisis de los sistemas internacionales existentes relacionados con el campo de acción no cumplen los requisitos funcionales que se desean, ni permiten la integración con el sistema xavia HIS, sin embargo sirvieron de base para identificar la dinámica de los diferentes sistemas analizados, así como las funcionalidades y una propuesta para la jerarquía de la aplicación.
- El modelado de los procesos del negocio permitió refinar las actividades manuales y definir las que se adicionarían al sistema.
- Se utilizó la arquitectura propuesta por el Centro de Informática Médica, además de las pautas establecidas, las cuales garantizaron la uniformidad visual de todas las interfaces del sistema.
- Las herramientas, tecnologías y patrones seleccionados permitieron crear un componente adaptable a diferentes entornos de trabajo. La implementación se basó en tecnologías de desarrollo libre, las cuales aseguraron la construcción de un sistema robusto, flexible y seguro.
- Con el producto obtenido se logró ampliar la calidad del xavia HIS, convirtiéndolo en un sistema más completo, mejorando el control del personal y de los activos en las instituciones de salud en tiempo real.

### Recomendaciones

En vista de mejorar las prestaciones del componente los autores recomiendan:

- ✓ Incorporar al componente un sistema de servicio de mensajes cortos (SMS, por sus siglas inglés) a móviles sobre determinados eventos que sean de interés, con el propósito de localizar de forma inmediata a cualquier directivo encargado del control de acceso y activos fijos de la entidad.

## Referencias Bibliográficas

1. **Freijedo, Claudio F, Cortagerena, Alicia B.** *Tecnologías de la información y las comunicaciones (2000)*. Buenos Aires, Argentina: Publicado por GJ Macchi, 2000, (2000).
2. **Tarjetas inteligentes.** [En línea] [Citado el: 25 de 5 de 2013.] [www.dhellas.com/cards.html](http://www.dhellas.com/cards.html).
3. **Sistema biométrico.** [En línea] [Citado el: 25 de 5 de 2013.]  
[http://www2.ing.puc.cl/~iing/ed429/sistemas\\_biometricos.htm&dt=-&s=-&r=DQE](http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm&dt=-&s=-&r=DQE).
4. **Portillo García, Javier I., Bermejo Nieto, Ana Belén and Bernardos Barbolla, Ana M.** *Tecnología de Identificación por Radiofrecuencia (RFID): aplicaciones en el ámbito de la salud*. Madrid: Fundación madrid para el Conocimiento, 2008.
5. **Idem Referencia 4.** [En línea]
6. **Sistema de Información Hospitalaria.** *México D.F.: Universidad Autónoma de México. D. R., 2003.* [En línea] [Citado el: 15 de 1 de 2013.] <http://www.facmed.unam.mx/emc/computo/ssa/HIS/his.pdf>.
7. **Guía de Seguridad.** [En línea] [Citado el: 15 de 1 de 2013.]  
[http://www.guiadelaseguridad.com.ar/canales\\_tecnicos\\_de\\_seguridad/control\\_de\\_accesos/33\\_acceso\\_a\\_domicilios.htm](http://www.guiadelaseguridad.com.ar/canales_tecnicos_de_seguridad/control_de_accesos/33_acceso_a_domicilios.htm).
8. **Tarjeta con cinta magnética.** [En línea] [Citado el: 25 de 5 de 2013.]  
[http://smtcc.en.alibaba.com/sellofferdetailshowimg/Sell\\_Magnetic\\_Card.html](http://smtcc.en.alibaba.com/sellofferdetailshowimg/Sell_Magnetic_Card.html).
9. **Código de barras.** [En línea] [Citado el: 25 de 5 de 2013.]  
<http://www.barcodeart.com/science/science.html>.
10. **Idem Referencia 2.** [En línea]
11. **Clave por teclado.** [En línea] [Citado el: 25 de 5 de 2013.] [www.olimpiahardware.com/access-control/index.html](http://www.olimpiahardware.com/access-control/index.html).
12. **Idem Referencia 5.** [En línea]
13. **SADOT, Alexandres, RODRIGUEZ-MORCILLO, Carlos y MUÑOZ, José.** *RFID: La tecnología de identificación por radiofrecuencia*. 2006.
14. **Blazquez del Toro, L.** *Sistemas de Identificación por Radiofrecuencia*. [En línea] [Citado el: 18 de 1 de 2013.] <http://www.it.uc3m.es/jmb/RFID/rfid.pdf>.
15. **Productos RFID.** [En línea] [Citado el: 15 de 10 de 2012.] <http://www.dipolerfid.es/Productos/Lectores-RFID/Default.aspx>.

16. **Castro, L & Foss Wamba, S.** *An inside look at RFID. Journal of Technology Management & Innovation.* 2007.
17. **LLRP Reader Control Simplified.** [En línea] [Citado el: 19 de 1 de 2013.] [www.impinj.com](http://www.impinj.com).
18. **Idem Referencia 17.** [En línea]
19. **Idem Referencia 5.** [En línea]
20. **Idem Referencia 5.** [En línea]
21. **MCM.** [En línea] [Citado el: 22 de 1 de 2013.] [http://www.mcm.es/cerraduras\\_electronicas\\_axess.php](http://www.mcm.es/cerraduras_electronicas_axess.php).
22. **UI Develoment with JaveServer Faces.** [En línea] [Citado el: 4 de 12 de 2012.] <http://www.itk.ilstu.edu/faculty/blim/itk353/j-jsf-ltr.pdf>.
23. **Hookom, Jacob.** JSF Central tm. Inside Facelets Part 1: An Introduction. [En línea] [Citado el: 2 de 2 de 2013.] [http://www.jsfcentral.com/articles/facelets\\_1.html](http://www.jsfcentral.com/articles/facelets_1.html).
24. **Ajax4jsf Developer Guide.** [En línea] 2007. [Citado el: 25 de 1 de 2013.] [http://www.jboss.org/file-access/default/members/jbossajax4jsf/freezone/docs/devguide/en/html\\_single/index.html](http://www.jboss.org/file-access/default/members/jbossajax4jsf/freezone/docs/devguide/en/html_single/index.html).
25. **Seamframework.** [En línea] 2009. [Citado el: 4 de 2 de 2013.] <http://seamframework.org>.
26. **Junta de Andalucía.** “Enterprise JavaBeans 3”. *Marco de Desarrollo de la Junta de Andalucía.* [En línea] 2 de 2012. [Citado el: 9 de 5 de 2013.] <http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/95>.
27. **JBoss Community.** Hibernate. [En línea] [Citado el: 28 de 1 de 2013.] <http://www.hibernate.org>.
28. **García de Jalón Javier, Rodríguez Iñigo Mingo José Ignacio, Alfonso Brazález Aitor Imaz, Larzabal Alberto, Calleja Jesús, García Jon.** *Aprenda Java como si estuviera en primero.* España: s.n, 2008.
29. **Java Platform, Enterprise Edition (JEE).** Oracle. [En línea] [Citado el: 6 de 2 de 2013.] <http://www.oracle.com/technetwork/java/javaee/documentation/index.html>.
30. **Idem Referencia 25.** [En línea]
31. **JBoss Server Manager Reference Guide.** Red Hat. [En línea] 2008. [Citado el: 19 de 1 de 2013.] <http://www.jboss.org/jbossas/docs>.
32. **PostgreSQL-es.** *Sobre PostgreSQL.* [En línea] 2010. [Citado el: 9 de 5 de 2013.] [http://www.postgresql-es.org/sobre\\_postgresql](http://www.postgresql-es.org/sobre_postgresql).
33. **Patricia López Martínez, Mario Aldea Rivas.** *Seminario de introduccion al entorno de desarrollo Eclipse.Programacion II.* 2011.

34. **Rifidi Prototyper**. [En línea] [Citado el: 9 de 5 de 2013.] <http://rifidi-prototyper.software.informer.com/1.0b/>.
35. **iReport**. [En línea] [Citado el: 9 de 5 de 2013.] <http://community.jaspersoft.com/wiki/ireport-designer-getting-started>.
36. **pgAdmin3**. [En línea] [Citado el: 9 de 5 de 2013.] <http://www.arpug.com.ar/trac/wiki/PgAdmin>.
37. **Visual Paradigm**. [En línea] [Citado el: 9 de 5 de 2013.] <http://www.visual-paradigm.com/product/vpuml>.
38. **Sommerville, Ian**. *Ingeniería del software. Séptima edición*. Madrid: Pearson Educación.
39. **Idem Referencia 39**. [En línea]
40. **Idem Referencia 39**. [En línea]
41. **Idem Referencia 39**. [En línea]
42. **Bascón Pantoja, Ernesto**. *El patrón de diseño Modelo-Vista-Controlador (MVC)*. 2004.
43. **Gutierrez, Jorge A. Saavedra**. El Mundo Informático. *PATRONES GRASP (Patrones de Software para la asignación General de Responsabilidad). Parte II*. [En línea] [Citado el: 2 de 3 de 2013.] <http://jorgesaaavedra.wordpress.com>.

---

## Bibliografía

1. **Ajax4jsf Developer Guide.** [En línea] 2007. [Citado el: 25 de 1 de 2013.] [http://www.jboss.org/file-access/default/members/jbossajax4jsf/freezone/docs/devguide/en/html\\_single/index.html](http://www.jboss.org/file-access/default/members/jbossajax4jsf/freezone/docs/devguide/en/html_single/index.html).
2. **Bascón Pantoja, Ernesto.** El patrón de diseño Modelo-Vista-Controlador (MVC). 2004.
3. **Blazquez del Toro, L.** Sistemas de Identificación por Radiofrecuencia. [En línea] [Citado el: 18 de 1 de 2013.] <http://www.it.uc3m.es/jmb/RFID/rfid.pdf>.
4. **Castro, L & Foss Wamba, S.** An inside look at RFID. Journal of Technology Management & Innovation. 2007.
5. **CESIM.** [En línea] [Citado el: 12 de 1 de 2013.] <http://gespro.cesim.prod.uci.cu/>.
6. **Clave por teclado.** [En línea] [Citado el: 25 de 5 de 2013.] [www.olimpiahardware.com/access-control/index.html](http://www.olimpiahardware.com/access-control/index.html).
7. **Código de barras.** [En línea] [Citado el: 25 de 5 de 2013.] <http://www.barcodeart.com/science/science.html>.
8. **Diccionario Economía - Administración - Finanzas - Marketing.** [En línea] [Citado el: 4 de 11 de 2013.] [http://www.eco-finanzas.com/diccionario/A/ACTIVO\\_FIJO.htm](http://www.eco-finanzas.com/diccionario/A/ACTIVO_FIJO.htm).
9. **Freijedo, Claudio F, Cortagerena, Alicia B.** Tecnologías de la información y las comunicaciones (2000). Buenos Aires, Argentina: Publicado por GJ Macchi, 2000, (2000).
10. **García de Jalón Javier, Rodríguez Iñigo Mingo José Ignacio, Alfonso Brazález Aitor Imaz, Larzabal Alberto, Calleja Jesús, García Jon.** Aprenda Java como si estuviera en primero. España: s.n, 2008.
11. **Guía de Seguridad.** [En línea] [Citado el: 15 de 1 de 2013.] [http://www.guiadelaseguridad.com.ar/canales\\_tecnicos\\_de\\_seguridad/control\\_de\\_accesos/33\\_acceso\\_a\\_domicilios.htm](http://www.guiadelaseguridad.com.ar/canales_tecnicos_de_seguridad/control_de_accesos/33_acceso_a_domicilios.htm).
12. **Gutierrez, Jorge A. Saavedra.** El Mundo Informático. PATRONES GRASP (Patrones de Software para la asignación General de Responsabilidad).Parte II. [En línea] [Citado el: 2 de 3 de 2013.] <http://jorgesaavedra.wordpress.com>.
13. **Hookom, Jacob.** JSF Central tm. Inside Facelets Part 1: An Introduction. [En línea] [Citado el: 2 de 2 de 2013.] [http://www.jsfcentral.com/articles/facelets\\_1.html](http://www.jsfcentral.com/articles/facelets_1.html).
14. **iReport.** [En línea] [Citado el: 9 de 5 de 2013.] <http://community.jaspersoft.com/wiki/ireport-designer-getting-started>.

- 
15. **Jacobson, Ivar, Booch, Grady and Rumbaugh, James.** El Proceso Unificado de Desarrollo. s.l.: Addison Wesley, 2000. SBN 84-7829-036-2.
  16. **Java Platform, Enterprise Edition (JEE).** Oracle. [En línea] [Citado el: 6 de 2 de 2013.] <http://www.oracle.com/technetwork/java/javaee/documentation/index.html>.
  17. **JBoss Community.** Hibernate. [En línea] [Citado el: 28 de 1 de 2013.] <http://www.hibernate.org>.
  18. **JBoss Server Manager Reference Guide.** Red Hat. [En línea] 2008. [Citado el: 19 de 1 de 2013.] <http://www.jboss.org/jbossas/docs>.
  19. **Junta de Andalucía.** "Enterprise JavaBeans 3". Marco de Desarrollo de la Junta de Andalucía. [En línea] 2 de 2012. [Citado el: 9 de 5 de 2013.] <http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/95>.
  20. **LLRP Reader Control Simplified.** [En línea] [Citado el: 19 de 1 de 2013.] [www.impinj.com](http://www.impinj.com).
  21. **López Hernández, Yurién Ing.** Desarrollo del Módulo Enfermería del Subsistema Web del Sistema Integral para la Atención Primaria de Salud alasSIAPS. La Habana: s.n., 2010.
  22. **MCM.** [En línea] [Citado el: 22 de 1 de 2013.] [http://www.mcm.es/cerraduras\\_electronicas\\_axess.php](http://www.mcm.es/cerraduras_electronicas_axess.php).
  23. **MILESTONE.** Curso UML, Cursos UML, UML Mexico-Milestone Consulting - Novedades. Curso práctico de Modelado de Negocios con BPMN 2.0 y UML. [En línea] 6 de 2002. [Citado el: 29 de 1 de 2012.] <http://www.milestone.com.mx/novedades.htm>.
  24. **Patricia López Martínez, Mario Aldea Rivas.** Seminario de introducción al entorno de desarrollo Eclipse. Programación II. 2011.
  25. **pgAdmin3.** [En línea] [Citado el: 9 de 5 de 2013.] <http://www.arpug.com.ar/trac/wiki/PgAdmin>.
  26. **Portillo García, Javier I., Bermejo Nieto, Ana Belén and Bernardos Barbolla, Ana M.** Tecnología de Identificación por Radiofrecuencia (RFID): aplicaciones en el ámbito de la salud. Madrid: Fundación Madrid para el Conocimiento, 2008.
  27. **PostgreSQL-es.** Sobre PostgreSQL. [En línea] 2010. [Citado el: 9 de 5 de 2013.] [http://www.postgresql-es.org/sobre\\_postgresql](http://www.postgresql-es.org/sobre_postgresql).
  28. **Productos RFID.** [En línea] [Citado el: 15 de 10 de 2012.] <http://www.dipolerfid.es/Productos/Lectores-RFID/Default.aspx>.
  29. **Rifidi Prototyper.** [En línea] [Citado el: 9 de 5 de 2013.] <http://rifidi-prototyper.software.informer.com/1.0b/>.
  30. **S, Presman Roger.** Ingeniería de Software, un enfoque práctico. s.l.: s.l.: McGraw-Hill, 2001, McGraw-Hill. 2001.

31. **SADOT, Alexandres, RODRIGUEZ-MORCILLO, Carlos y MUÑOZ, José.** RFID: La tecnología de identificación por radiofrecuencia. 2006.
32. **Seamframework.** [En línea] 2009. [Citado el: 4 de 2 de 2013.] <http://seamframework.org>.
33. **Sistema biométrico.** [En línea] [Citado el: 25 de 5 de 2013.] [http://www2.ing.puc.cl/~iing/ed429/sistemas\\_biometricos.htm&dt=-&s=-&r=DQE](http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm&dt=-&s=-&r=DQE).
34. **Sistema de Información Hospitalaria.** México D.F.: Universidad Autónoma de México. D. R., 2003. [En línea] [Citado el: 15 de 1 de 2013.] <http://www.facmed.unam.mx/emc/computo/ssa/HIS/his.pdf>.
35. **Sommerville, Ian.** Ingeniería del software. Séptima edición. Madrid: Pearson Educación.
36. **Tarjeta con cinta magnética.** [En línea] [Citado el: 25 de 5 de 2013.] [http://smtcc.en.alibaba.com/sellofferdetailshowimg/Sell\\_Magnetic\\_Card.html](http://smtcc.en.alibaba.com/sellofferdetailshowimg/Sell_Magnetic_Card.html).
37. **Tarjetas inteligentes.** [En línea] [Citado el: 25 de 5 de 2013.] [www.dhellas.com/cards.html](http://www.dhellas.com/cards.html).
38. **UI Develoment with JaveServer Faces.** [En línea] [Citado el: 4 de 12 de 2012.] <http://www.itk.ilstu.edu/faculty/bllim/itk353/j-jsf-ltr.pdf>.
39. **Visual Paradigm.** [En línea] [Citado el: 9 de 5 de 2013.] <http://www.visual-paradigm.com/product/vpuml>.

### Glosario de términos

**Activo:** es un bien tangible o intangible que posee una empresa o persona natural. Por extensión, se denomina también al conjunto de los activos de una empresa.

**Activo fijo:** son los bienes que una empresa utiliza de manera continua en el curso normal de sus operaciones; representan al conjunto de servicios que se recibirán en el futuro a lo largo de la vida útil de un bien adquirido.

**Activos fijos tangibles (AFT):** representan propiedades físicamente tangibles que han de utilizarse por un período largo en las operaciones regulares de la entidad y que normalmente no se destinan a la venta.

**Caso de uso:** secuencias de acciones que el sistema puede llevar a cabo interactuando con sus actores, incluyendo alternativas dentro de las secuencias.

**Eficiencia:** capacidad de disponer de alguien o de algo para conseguir un objetivo determinado.

**Entendimiento:** las actividades que reciben requisitos los analizan con los proveedores con el objetivo de asegurar que se llegue a un entendimiento común sobre el significado de los requisitos.

**Expediente de proyecto:** conjunto de documentos y plantillas estructura siguiendo una jerarquía que constituyen referencia para la documentación de los proyectos de la Universidad de las Ciencias Informáticas.

**Informática:** disciplina que estudia el tratamiento automático de la información utilizando dispositivos electrónicos y sistemas computacionales.

**Requisito:** (1) Una condición o capacidad necesitada por el usuario para resolver un problema o lograr un objetivo. (2) Una condición o capacidad que debe poseer un producto o componente de producto para satisfacer un contrato, estándar, especificación, u otros documentos obligatorios formales. (3) Una representación documentada de una condición o capacidad como en (1) o (2).

**Servicio:** unidad de software que encapsula alguna funcionalidad de negocio y proporciona estas a otros servicios a través de interfaces públicas bien definidas.

**Software:** conjunto de programas y procedimientos necesarios para hacer posible la realización de una tarea específica, en contraposición a los componentes informáticos físicos del sistema.

**Transpondedores:** es un tipo de dispositivo utilizado en telecomunicaciones cuyo nombre viene de la fusión de las palabras inglesas *Transmitter* (Transmisor) y *Responder* (Contestador/Respondedor). Se designa con este término (o con alguna de las abreviaturas XPDR, XPNDR, TPDR o TP) a equipos que realizan la función de:

- Recepción, amplificación y reemisión en una banda distinta de una señal (estos transpondedores se utilizan en comunicaciones espaciales para adaptar la señal satélite entrante/saliente a la frecuencia de los equipos en banda base).
- Respuesta automática de un mensaje (predeterminado o no) a la recepción de una señal concreta de interrogación (estos transpondedores se utilizan en aeronáutica para sistemas de pseudo-radar).

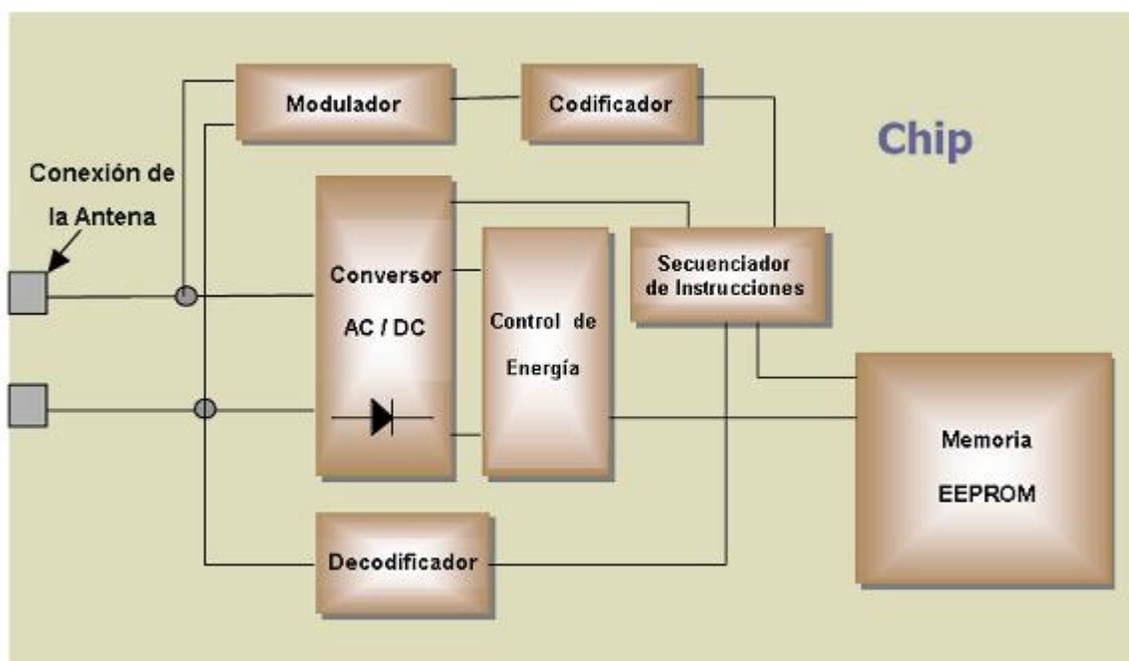
**Reglas de Negocio:** las reglas del negocio describen las políticas, normas, operaciones, definiciones y restricciones presentes en una organización y son de vital importancia para alcanzar sus objetivos.

**Usabilidad:** hace referencia, a la rapidez y facilidad con que las personas llevan cabo sus tareas propias a través del uso del producto objeto de interés.

## Anexos



## Anexo 1. Ejemplos de etiquetas



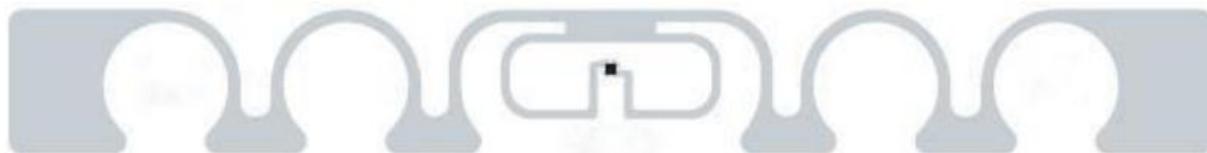
## Anexo 2. Arquitectura de una etiqueta



**Anexo 3. Lectores UHF**



**Anexo 4. Equipos propuestos: Alien 915 MHz Antena Circular ALR-9611-CR**



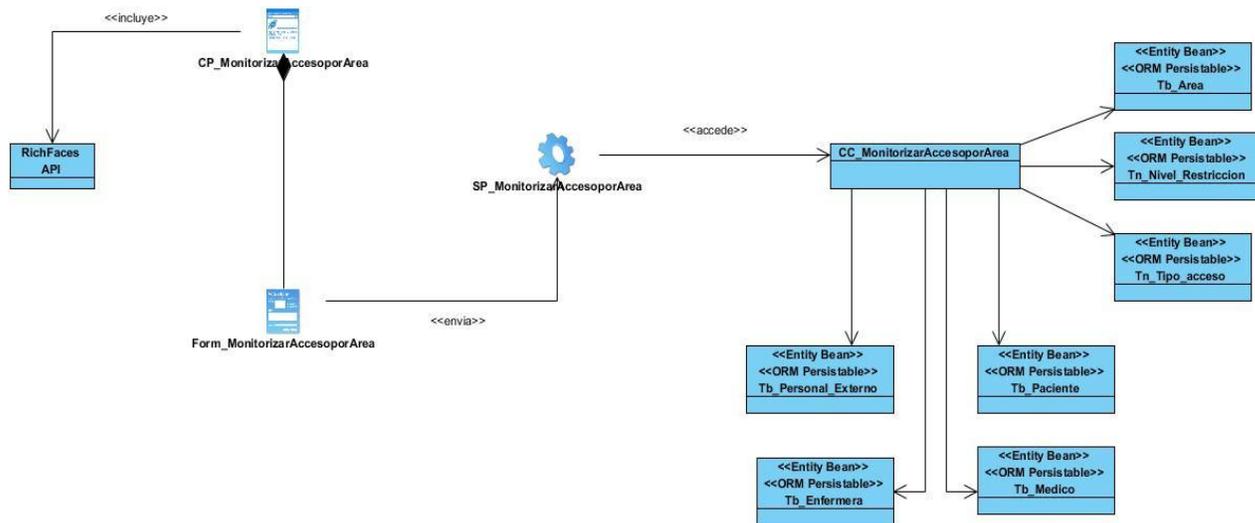
**Anexo 5. Equipos propuestos: Etiqueta 115004 Ultra Alta Frecuencia**



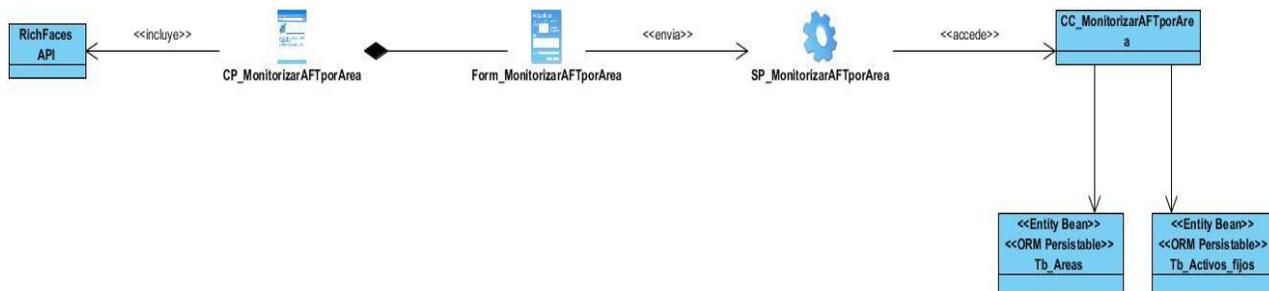
**Anexo 6. Equipos propuestos: Lector 216010 Gen2 de largo alcance**



**Anexo 7. Equipos propuestos: Lector USB RFID UHF de escritorio**



Anexo 8. Diagrama de Clases del Diseño: DCD\_Monitorizar Acceso por Area



Anexo 9. Diagrama de Clases del Diseño: DCD\_Monitorizar AFT por Area



Anexo 10. Diagrama de Clases del Diseño: DCD\_Quitar Acceso del Personal