UNIVERSIDAD DE LAS CIENCIAS INFORMATICAS
DIP SEGURIDAD Y PROTECCION FISICA

SISTEMA DE CONTROL DE ACCESO

Trabajo de Diploma para optar por el Título de Ingeniería Informática

Autor:

Miguel de Jesús Orama Fernández

Tutor:

Ing. Yailet Martínez Pérez

Ciudad de la Habana
Junio de 2004

RESUMEN

La Universidad de las Ciencias Informáticas (UCI) por tener características especiales tiene en sus manos una misión muy importante, que es la de desarrollar la industria del software cubano, con ese fin, la Revolución ha puesto en sus manos los medios con los que podremos construir nuestro futuro y el del país. Para lograr esto, es también necesario tomar medidas de seguridad y protección para proteger estos medios y velar por la seguridad.

Con la integración de diferentes sistemas, como, el de Acreditación, el de Control de Visitantes y el de Reservación de Pase, pueden ser automatizados muchos procesos que se realizan manualmente, generación automática de reportes con las horas de entrada y salida del personal de la Universidad, detección casi inmediata de ausentismo, retardos, violaciones de seguridad, datos estadísticos y otras facilidades.

INDICE

Introducción

La Universidad de las Ciencias Informáticas (UCI), específicamente la Dirección Integrada de Proyectos (DIP) de Seguridad y Protección Física ha decidido desarrollar e implementar una aplicación que controle la entrada y salida del personal a la UCI y a sus instalaciones para así resolver esta situación en cierta medida.

El sistema para el Control de Acceso lo desarrollará el Dpto. de Seguridad y Protección basándose en el Proceso Unificado de Software (RUP) y utilizando el Lenguaje de Modelado (UML) ya que cuentan con personal capacitado para ello y valiéndose de un sistema de Acreditación implantado donde están almacenado los datos de identificación de todo el personal de la Universidad, esto hace posible la implementar un sistema de Control de Acceso por contar con esta infraestructura informativa en materia de información personal.

Los carnet de identificación que posee todo el personal llevan algunos datos como son: el nombre, apellidos, la clasificación de esta, con una letra y por colores, número de solapín y código de barras, y en estos dos últimos datos basaremos la identificación de cada persona, es decir, la captura de datos del sistema de Control de Acceso será mediante un lector de código de barras o la introducción manual del número del solapín de la persona por parte de los Agentes de Seguridad en los puntos de Acceso a la UCI que es donde se operará este sistema. Estos valores, el número de solapín y el código de barras, no se repiten y son de clave única, respectivamente.

Este sistema de Control de Acceso podrá "identificar" a las personas mediante el ingreso de su código de barras o su número de solapín, permitir el acceso o denegarlo y registrar las entrada y salida de las personas a la UCI; así como detectar posibles violaciones de sus seguridad y/o la posible entrada de personas ajenas al centro sin autorización.

El Sistema de Control de Acceso formará parte de toda una estructura organizativa para la gestión interna de la Universidad. Entre estos sistemas se encuentran: el Sistema de

Acreditación, Sistema de Reservación de Pase (para los estudiantes) y que se relacionan fuertemente con este, son los sistemas de Control de Visitantes y de Control de Asistencia.

CAPITULO I

FUNDAMENTACIÓN TEÓRICA

1.1 Introducción

En este capítulo, Capítulo I: Fundamentación Teórica, son tratados temas referentes al Control de Acceso, sus inicios, la tecnología empleada para llevar a cabo el control de acceso, a qué se le controlará el acceso, por qué, los métodos para capturas los datos, ventajas y desventajas, serán objetos de comparación las tecnologías punteras del mercado en este sector y su incidencia y relación con otros sistemas.

1.2 Estado del Arte

Históricamente, las sociedades y el ser humano han tenido la necesidad de controlar el acceso a ciertas áreas y lugares. Esta necesidad es motivada inicialmente por temor que personas inescrupulosas o delincuentes puedan robar y/o extraer material valioso de acuerdo a criterios personales, sociales o comerciales. Vemos cómo los castillos y fortalezas fueron construidos de tal forma que sus principales vías de acceso eran diseñadas con puentes que se elevaban o recogían mediante mecanismos manuales, quedando así abajo un círculo de agua y caimanes que rodeaban dicho castillo o fortaleza. En tal sentido, el acceso a estas edificaciones no sólo era posible suministrando un nombre. En efecto, las palabras claves o contraseñas, eran utilizadas por pocas personas para acceder al castillo. Este no fue el único mecanismo de seguridad de acceso, también se debía hacer un reconocimiento visual de las características de ella/él o de un único elemento, como por ejemplo un anillo.

Bien se ha dicho que nos encontramos en la Era de la Informática y las Telecomunicaciones, donde, la Información domina. Los datos se encuentran codificados en casi cualquier sitio, tarjetas telefónicas, tarjetas magnéticas, tarjetas inteligentes y códigos de barras.

Si UD mira un momento a su alrededor, seguro encontrará algún código de barras en algún objeto cercano a UD, puede haber incluso varios y se ha preguntado alguna vez como funcionan y para que se utilizan los códigos de barras.

En la actualidad son muchas las razones por la que empresas e instituciones, lo mismo requieren de controlar el acceso a sus instalaciones, las más comunes son: para lograr una mayor seguridad y para controlar y registrar los horarios de entrada y salida de las personas a su jornada laboral. Estas son las razones fundamentales como para que sea implantado un sistema de control de acceso.

Una variada gama de modelos posibilita brindar una solución efectiva tanto en las grandes empresas que requieren máxima seguridad, robustez y flexibilidad de

programación, como en pequeños comercios que necesitan precios económicos y facilidad de uso. Un software de control de acceso, con sus accesorios en cada caso, permiten llevar el control de horarios a lugares en los cuales antes no era posible por cuestiones de costo u operativas (oficinas remotas, obras, personal móvil e inspectores, etc.) y fueron pensados de manera de adaptarse a todas las necesidades del mercado.

El reto, entonces, es encontrar esa solución que garantice una relación costo/beneficio y que requiera la menor cantidad de esfuerzo en su implantación y uso.

La captura de datos de tarjetas magnéticas, tarjetas de proximidad, código de barras y biométricos, le explicaremos a continuación así como el funcionamiento estos sistemas de control de accesos, en dependencia de la tecnología que se esté usando, para identificar a las personas, permitir el acceso o no y registrar el horario de sus accesos.

A lo largo de este capítulo trataremos de aclarar algunas de estas interrogantes, vayamos por partes.

1.3 Sistemas de Control de Acceso

En primer lugar es necesario conocer cuáles son esos diferentes tipos de Lectores y Tarjetas, analizando los pro y los contra de cada uno.

Los sistemas de Control de Acceso usan estas tecnologías que son las más conocidas y utilizadas:

- ✓ Claves por Teclado
- ✓ Tarjetas de Banda Magnética
- ✓ Tarjetas de Código de Barras
- ✓ Touch Memory
- ✓ Tarjetas de Proximidad ó Radio Frecuencia (RF)
- ✓ Biométricos.

1.3.1 Claves por Teclado

Realmente 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.

1.3.2 Tarjetas de Banda Magnética

Es la tecnología más conocida y difundida, dado que se utiliza en todos los sistemas de tarjetas de crédito y de compra (de hecho se pueden utilizar esas mismas tarjetas en muchos sistemas de Control de Acceso). Su ventaja es su difusión, popularidad y el bajo costo, pero en sí es, de todos los medios de identificación, el más vulnerable de todos. La banda magnética de la tarjeta, debe ser tratada con cierto cuidado, para evitar que se raye o sea expuesta a campos magnéticos que la borren, por tal motivo, no son recomendables para usar en ambientes industriales.
Sólo se recomiendan en oficinas o establecimiento administrativos.
En relación con el lector en sí, es también de los más económicos, pero posee un cabezal magnético, el cual sufre cierto desgaste al pasar las tarjetas por el lector. En realidad cada tarjeta que se pasa, deja micropartículas depositadas sobre la cabeza lectora. Ahora bien, si esas partículas son abrasivas, comienzan a rayar las tarjetas sucesivas y las tarjetas rayadas o rotas, deterioran aun más el cabezal, obligando al recambio del lector y de las tarjetas dañadas. El tiempo de duración, depende exclusivamente del ambiente, frecuencia de uso y el trato con el que se los utilice.

1.3.3 Tarjetas de Código de Barras

Las tarjetas de Códigos de Barras son de apariencia similar a las magnéticas, pero en lugar de la banda, llevan impreso un código de barras, el cual puede incluso ser protegido con una banda protectora (código oculto) que evita la duplicación de la tarjeta por fotocopias. La ventaja de esta tarjeta, es que al pasarla por el lector, no existe rozamiento con un cabezal, sólo hay un haz de luz que lee el código en cuestión, con lo cual su vida útil es mayor, pero tampoco se pueden rayar, porque

de esa forma se altera o incluso llega a hacerse ilegible el código, obligando al cambio de tarjeta. El costo de las tarjetas es similar a las magnéticas.

Los lectores que se utilizan en los equipos de Control de Acceso y Presentismo pueden ser de diferentes calidades y prestaciones. El otro punto fundamental es que el lector permita leer no solo las tarjetas con códigos visibles, sino también las tarjetas con código protegido, por lo que ya comentamos acerca de la posibilidad de duplicarlas.

1.3.4 Touch Memories

El elemento en sí es una pastilla electrónica, encapsulada en acero inoxidable de unos 16 mm. de diámetro, que se transportan con un soporte plástico de unos 5 cm. de largo con un ojalillo en su parte superior para poder colgarlo en un llavero. En caso de necesitar usarlo como credencial, también se los puede pegar sobre tarjetas de PVC idénticas a las otras.

Comúnmente se los denomina llave electrónica y brindan un muy alto nivel de seguridad, ya que son altamente resistentes al desgaste, siendo ideales para ambientes industriales en donde la probabilidad de falla, vandalismo o sabotaje sea alta, aunque no son recomendables para ambientes con alto grado de generación de corriente estática (P. Ej.: oficinas con mucha alfombra y ambientes muy secos). Su tecnología de avanzada evita la posibilidad de duplicarlas. En precio hay que tener en cuenta que son unos de los medios más caros, aunque en relación, nunca se desgastan, como puede suceder con una tarjeta magnética, dado que en lo que al lector respecta es también de acero inoxidable y por ende no tiene desgaste con el uso.

1.3.5 Proximidad o Radio Frecuencia (RF)

Un sistema de RF consta de dos partes; 1) La unidad lectora y 2) El tag, transponder o tarjeta. Cuando la tarjeta posee alimentación interna, se la denomina proximidad activa y cuando la tarjeta no tiene esa batería interna se la denomina proximidad

pasiva. Mayoritariamente son utilizados los sistemas de proximidad pasiva. El lector emite una onda electromagnética que se propaga en el aire. La onda tiene forma elíptica, en la cual el lector queda en medio de ella.

Ese campo electromagnético genera, cuando una tarjeta entra en el mismo, instantáneamente una corriente interna, que sirve para alimentar a la misma. Dentro de la tarjeta existe un microchip que posee: una memoria que guarda los bits de datos con el código de la misma; una antena que es la encargada de recibir y transmitir.

Al inducirse esa corriente en la tarjeta, la misma extrae de la memoria el dato codificado y lo devuelve, enviándolo al lector por la misma onda electromagnética. El lector lo recibe, lo decodifica, lo filtra, lo amplía y lo envía a la Unidad de Control de Accesos a la que esté conectada.

Es una tarjeta que por su diseño tecnológico, es prácticamente imposible que pueda duplicarse. Hoy en día es una de las tecnologías más moderna y efectiva, por su practicidad y bajo costo de mantenimiento.

1.3.6 Biométricos

Su funcionamiento se basa en la lectura o reconocimiento de alguna parte del cuerpo humano; de la huella dactilar, geometría de la mano, de la voz, por la retina o iris y reconocimiento facial; 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 nadie puede entregarle o pedirle a otra persona la "tarjeta para fichar", pero hasta el momento siguen luchando para resolver varios puntos que complican su entrada masiva al mercado.

El más importante pasa por el precio del lector, y le siguen la velocidad de lectura (comúnmente son bastante lentos o deben ir acompañados de un teclado para anteponer un código para acelerar el proceso de búsqueda), y por último la poca

posibilidad de ser autónomos (generalmente por su complicada lógica se ven obligados a trabajar con un software de análisis y una PC conectada directa al lector, lo cual es poco versátil y más caro aún), pero seguramente con el tiempo se irán superando estas dificultades y en un futuro de mediano plazo, llegarán a ser un standard más.

A continuación una pequeña comparación de las tecnologías más usadas en el mercado que haremos teniendo en cuenta ciertos aspectos. Ver Anexo 2.

1.4 ¿Cómo funcionaban y aún funcionan muchas empresas?

Los sistemas antiguos de control de tiempo trabajado, eran manuales, a base de relojes chequeadores mecánicos y tarjetas reloj, haciendo muy lento y trabajoso disponer de esta información. Una vez que las tarjetas se encuentran preparadas se colocan en los tarjeteros respectivos. Los empleados registran sus entradas y salidas diarias en estas tarjetas y son revisadas y corregidas diariamente por una secretaria o supervisor. Al final del período deben de ser revisadas nuevamente. Finalmente, los capturistas dan entrada a esta información al sistema de nómina. Este procedimiento consume tiempo de capturistas, personal de nóminas e incluso gerentes, en preparar y revisar las asistencias de los empleados. Como todo sistema manual, está expuesto a vulnerabilidad de los registros de entrada y salida, así como errores en la captura de esta información.

En los sistemas de Control de Acceso actuales los códigos de barras pueden ser leídos de muchas formas usando diferentes dispositivos. Generalmente un sistema de lectura se compone de dos partes: una interfaz, llamada por lo regular "decodificador", y lo que se conoce con el poco llamativo término de "dispositivo de entrada". Toda la magia tiene lugar en el decodificador. El trabajo del dispositivo de entrada casi pasa desapercibido, mientras que el decodificador ejecuta las labores sofisticadas. En algunas ocasiones, estos dos elementos están interconstruídos y forman una sola unidad. Esto es, la decodificación se realiza dentro del dispositivo de entrada y no en un equipo externo.

Existen básicamente tres maneras de poner a estos dos elementos a trabajar juntos para leer códigos de barras. Estos métodos se conocen como Sistemas En Línea, Sistemas Fuera de Línea (o "batch") y Sistemas de RF (radio frecuencia).

1.4.1 Sistemas en Línea

Estos sistemas están conectados de una manera semi-permanente a una computadora o terminal. Su función principal es leer un código de barras, interpretarlo (decodificarlo) y transmitirlo inmediatamente. Por lo general, los sistemas En Línea toman dos formas: conexión directa a teclado o "wedge", conexión serial y tarjeta de expansión. La conexión "wedge" se utiliza principalmente en microcomputadoras (IBM PC, Apple y compatibles), así como en terminales de sistemas de cómputo de IBM. El "wedge" provee una conexión directa entre el lector de código de barras y el teclado de la PC o terminal.

Todos estos sistemas trabajan de la misma manera, cambiando la señal analógica que les envía el lector, convirtiéndola y haciéndola parecer a la computadora como información tecleada. Por lo tanto, todos los sistemas En Línea son, esencialmente, un segundo teclado para la computadora. No se requiere de software o drivers adicionales, ya que la interfaz se hace vía hardware.

Los sistemas En Línea son programables, por lo general leyendo comandos codificados en código de barras impresos en el manual que se incluye con estos equipos. Todos los parámetros se almacenan en la memoria no volátil del decodificador, y la única manera de cambiarlos es leyendo nuevos comandos que modifiquen la configuración existente. ¿Por qué razón se querría programar un decodificador? Bien, por ejemplo, se puede requerir que se envíe un "enter" automáticamente después de cada lectura, o bien que se transmitan códigos de teclados de computadoras tipo XT en lugar de AT. Con ciertos equipos, actualmente es posible editar, separar o filtrar la información del código de barras antes de enviarlo al sistema de cómputo.

1.4.2 Sistemas Fuera de Línea

Mientras que un Sistema En Línea requiere que el operador esté a unos cuantos centímetros de la terminal, los Sistemas Fuera de Línea abren todo un nuevo horizonte de aplicaciones. Estos sistemas se pueden considerar como un computadora portátil y un lector de código de barras trabajando en conjunto y se conocen como Terminales Portátiles de Datos (PDT, por "Portable Data-entry Terminals"), Terminales Manuales o simplemente Asistentes Personales (PDA, Personal Digital Assistant) generalmente tipo Palm Pilot. Por lo general operan con baterías recargables y pesan menos de 1 Kg.

Los sistemas portátiles vienen en dos presentaciones diferentes: no-integrados e integrados. En el primer caso, la computadora portátil y el lector son dos componentes separados, conectadas mediante un cable. En el segundo, el lector y la computadora están interconstruídos en una misma unidad.

Los sistemas portátiles se pueden concebir de dos maneras: como simples dispositivos de recolección de datos o como extensiones del sistema de cómputo con más capacidad de procesamiento que sólo almacenar la información capturada. Originalmente, debido a herramientas de programación menos desarrolladas, sistemas operativos anticuados y falta de memoria, las terminales portátiles funcionaban como unidades de almacenamiento para tomas de inventario o encuestas. Ahora, con MB de RAM, sistemas operativos ampliamente conocidos (como DOS) y poderosos lenguajes de programación, las terminales portátiles son prácticamente tan poderosas como las computadoras de escritorio.

1.4.3 Sistemas de Radiofrecuencia (RF)

Esencialmente, estos sistemas son terminales portátiles con un transmisor y receptor de radiofrecuencia integrado en el equipo. Estas unidades proveen lo mejor de dos mundos ya que están conectadas en línea al sistema de cómputo manteniendo la libertad de movimiento y portabilidad, aún operando a cientos de metros del "host". Actualmente hay dos tecnologías que compiten en el mercado de RF: Banda Angosta ("narrow band") y Espectro Extendido ("spread spectrum"). La primera es la más tradicional, requiriendo el uso de una frecuencia exclusiva en el área geográfica de cobertura y una licencia gubernamental. Los sistemas más recientes utilizan Espectro Extendido, no requieren de licencia y se asemejan a la tecnología celular utilizada en la telefonía móvil.

1.5 Códigos de Barras

Los códigos de barras son una forma óptica para almacenar información reconocible por los sistemas informáticos.

Cada vez más y más aplicaciones que usan los códigos de barras para identificar medios, productos, inventarios, en fin muchas cosas con el fin de poderlas identificar y controlar, pero quizás los más conocidos son los usados para identificar productos de consumo y por supuesto.

La tecnología de código de barras es una de punta en el mercado, sobre todo muy económica, y de fácil implementación, ya que con una impresora de calidad pueden ser impresos los carnets de identificación con códigos de barras. Podemos chequear algunos aspectos sobre las tecnologías de punta en el mercado.

Esta tecnología es más eficiente que las de banda magnética, por ejemplo, por su dificultad de duplicación y que son con clave única, lo que las hace más confiables, in dependientemente que las de banda magnética pueden “desmagnetizarse” producto el roce y el desgaste del proceso de las lecturas. Aunque los carnets que usan códigos de barras pueden ser falsificados porque una fotocopia de este funcionaría en el momento

de la identificación, esto puede ser evitado con una banda protectora del código de barras, así estaría "protegido" contra fotocopias pero puede ser leído igual por los lectores de código de barras.

No sólo los medios o productos son controlables o identificables, también puede ser que una institución o empresa requiera una credencial o identificación para sus empleados o miembros. Este es el caso de la Universidad de la Ciencias Informáticas (UCI) y el tema que nos ocupa: el Control de Acceso a la UCI.

La UCI tiene implementado un Sistema de Acreditación, en este se encuentran almacenada la información de todo su personal. Este cuente con un carnet (o solapín) que tiene algunos datos del propietario: nombre, apellidos, número de solapín, foto y un *código de barras* impreso en el reverso. En la actualidad muchos servicios que se prestan en la UCI requieren de la autentificación mediante este carnet. El sistema de control de Acceso requiere que todo el personal posea dicha identificación para llevar a cabo los propósitos del sistema: identificar, controlar la entrada y salida de las personas a la UCI y registrar estos eventos.

Para esto es preciso que UD. lector, posea una idea general de la capacidad, las ventajas y desventajas de sólo una de estas simbologías que es la que trataremos en este trabajo.

1.5.1 Breve Historia de su Desarrollo

Todo empezó en EEUU, en 1970, cuando se empezó a pensar en un sistema capaz de resolver los problemas informáticos que surgían en todas aquellas actividades industriales y comerciales que manipulan una gama muy amplia de productos en grandes cantidades y tenían verdaderos problemas en la aplicación de los sistemas informáticos debido a la ardua labor de codificación necesaria para la introducción de los artículos de movimientos. Estas entidades empleaban un gran número de personas especializadas y entrenadas en la introducción de datos en los ordenadores.

En grandes supermercados, por ejemplo, cada artículo había de identificarse mediante la colocación de una etiqueta adhesiva con un número de código y después, al ser introducido en el ordenador, era relacionado con el nombre, descripción y precio del producto, con vistas a su facturación y control en los inventarios. Se tenía que encontrar una solución para facilitar la introducción de datos en el ordenador, de forma que no se precisara personal especializado y fuera "segura" donde no interviniera el error humano en la captura e introducción de los datos al ordenador.

Como solución a toda esta problemática se ha desarrollado el código de barras que, cumpliendo todos esos requisitos, se va imponiendo en la mayoría de mercados del mundo.

En principio se pensó para la industria farmacéutica por sus especiales características de gran cantidad de artículos y necesidad de rotación de inventarios.

En 1973 se publicaron las primeras normas y standards bajo la denominación de Universal Product Coding (UPC). El sistema suponía la creación de un banco de números en el que se registraba el número asignado a cada fabricante. Después, el fabricante daba el número del producto, el cual se ponía en la segunda mitad del código, detrás del número del fabricante.

Aunque al principio se acogió el sistema con cierto entusiasmo, enseguida empezaron a aparecer algunos problemas de tipo laboral al creer los sindicatos que su implantación podría afectar al empleo. Por su parte, los minoristas se mostraban poco dispuestos a hacer la inversión necesaria en la compra de equipos de lectura. Incluso los consumidores se mostraban partidarios de ver los precios individuales en cada artículo.

A pesar de ello, algunos fabricantes se mostraron muy decididos a seguir adelante y marcaron sus productos con el con el código de barras UPC. Las críticas negativas desaparecieron.

El hecho de que el código de barras permitía una facturación más rápida a la salida de los supermercados y que el recibo o ticket daba una información muy detallada de la

compra, convenció a los consumidores en el sentido de preferir los establecimientos que trabajan con el nuevo método. Tanto fue así que los minoristas que lo adoptaron vieron crecer sus ventas notablemente.

Cuando los resultados obtenidos fueron publicados y los aparatos de lectura se ofrecieron a precios más asequibles, la mayoría de cadenas de establecimientos se decidieron a utilizar el sistema, popularizándose a nivel general.

Esa aceptación general en EEUU ocurría hacia 1977. Fue entonces cuando Europa planteó la misma problemática. Algunos empresarios lo ensayaron primero para adoptarlo definitivamente después.

El código empleado en Europa, es distinto y más empleado que el americano. Se le conoce por European Article Numering o por las siglas EAN. Empezó en 1977 y en el Reino Unido se inició en el sistema en 1978. En el Reino Unido existe desde entonces la Article Numering Association (ANA) que encarga de coordinar los códigos. Después otros países, entre ellos España, se han adherido.

1.5.2 Tipos de Códigos de Barras

Los Código de Barras puede incluso ser protegido con una banda protectora (código oculto) que evita la duplicación de la tarjeta por fotocopias. La ventaja de esta tarjeta, es que al pasarla por el lector, no existe rozamiento con un cabezal, sólo hay un haz de luz que lee el código en cuestión, con lo cual su vida útil es mayor, pero tampoco se pueden rayar, porque de esa forma se altera o incluso llega a hacerse ilegible el código, obligando al cambio de tarjeta. Los lectores que se utilizan en los equipos de Control de Acceso y Asistencia pueden ser de diferentes calidades y prestaciones.

El otro punto fundamental es que el lector permita leer no sólo las tarjetas con códigos visibles, sino también las tarjetas con código protegido, por lo que ya comentamos acerca de la posibilidad de duplicarlas.

Estos son los codificadores de los códigos de barras más utilizados actualmente:

- Código 39
- Código 39 ASCII Total
- Codabar
- Intercalado 2 de 5
- Código 128
- UPC (Código Universal de Producto)
- EAN (European Article Numbering o Sistema de Numeración Europeo)

1.5.3 Beneficios

Los beneficios son incontables en dependencia de la cantidad de aplicaciones donde se pueden implementar los códigos de barras.
Reduce los costos de tiempo y recursos que haciendo los procesos manualmente y se disminuye considerablemente la introducción del error humano en los procesos de captura de los datos y procesamiento de información.
En materia de seguridad, aumenta el nivel de seguridad de los lugares donde estén instalados estos sistemas.

1.5.4 Aplicaciones

Las aplicaciones del código de barras cubren prácticamente cualquier tipo de actividad humana, tanto en industria, comercio, instituciones educativas, instituciones médicas, gobierno, etc., es decir, cualquier negocio se puede beneficiar con la tecnología de captura de datos por código de barras, tanto el que fabrica, como el que mueve, como el que comercializa.

Entre las aplicaciones que tiene podemos mencionar:

- ✓ Control de material en procesos
- ✓ Control de inventario
- ✓ Control de movimiento

- ✓ Control de tiempo y asistencia
- ✓ Control de acceso
- ✓ Punto de venta
- ✓ Control de calidad
- ✓ Control de embarques y recibos
- ✓ Control de documentos y rastreos de los mismos
- ✓ Rastreos preciso en actividades
- ✓ Rastreos precisos de bienes transportados
- ✓ Levantamiento electrónico de pedidos
- ✓ Facturación
- ✓ Bibliotecas

1.5.5 Codificación utilizada en la UCI: Código 39

En la UCI ya se encuentra implantado un sistema de Acreditación, por lo que todas las personas de la UCI cuentan con un carnet que los identifica, como hemos dicho anteriormente, el código de barras de los carnets de identificación es el Código 39, veámoslo al detalle.

La simbología Código 39 es actualmente la más usada para aplicaciones industriales y comerciales. Permite la codificación de caracteres numéricos, así como letras mayúsculas y algunos símbolos como -, ., $, /, +, % y "espacio". Un símbolo puede codificar uno o muchos caracteres, con una posibilidad de error de sustitución muy baja. Se utilizan sólo dos grosores tanto para barras como para espacios.

Aunque es muy confiable, el Código 39 no es muy denso, ya que se requieren muchas barras y espacios para representar un sólo caracter. Aunque esto rara vez representa un problema, ocasionalmente símbolos muy largos pueden exceder el tamaño de la etiqueta.

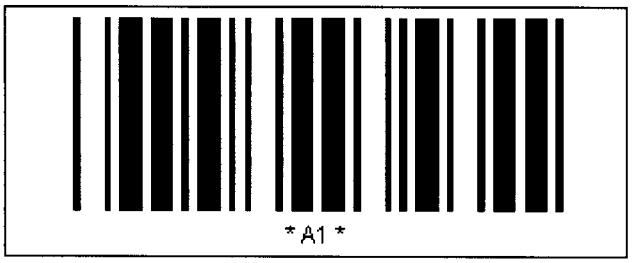


Figura 1.1 Tipo de codificación Código 39.

1.5.6 Tipos de Lectores

Los códigos de barras pueden ser leídos de muchas formas usando diferentes dispositivos. Generalmente un sistema de lectura se compone de dos partes: una interfaz, llamada por lo regular "decodificador", y lo que se conoce con el poco llamativo término de "dispositivo de entrada". Toda la magia tiene lugar en el decodificador. El trabajo del dispositivo de entrada casi pasa desapercibido, mientras que el decodificador ejecuta las labores sofisticadas.

En algunas ocasiones, estos dos elementos están empotrados y forman una sola unidad. Esto es, la decodificación se realiza dentro del dispositivo de entrada y no en un equipo externo. Existen básicamente tres maneras de poner a estos dos elementos a trabajar juntos para leer códigos de barras. Estos métodos se conocen como Sistemas En Línea, Sistemas Fuera de Línea (o "batch") y los sistemas de Proximidad o Radio Frecuencia.

Los ***lectores tipo pluma o lápiz*** son definitivamente los más populares. Esto se debe principalmente a su bajo precio, fácil reemplazo, durabilidad y portabilidad. Para usarlo apropiadamente, el operador coloca la punta del lector en la zona blanca que está al inicio o final del código y lo desliza a través del símbolo a velocidad e inclinación constante. Los lectores tipo pluma requieren de cierta habilidad por parte del usuario, y sólo son prácticos cuando se leen códigos colocados en superficies duras, planas y de preferencia horizontales.

Los ***lectores de ranura (o "slot")*** son básicamente lectores tipo pluma montados en una caja. La lectura se realiza al deslizar una tarjeta o documento con el código de barras impreso cerca de uno de sus extremos por la ranura del lector. La probabilidad de leer el código en la primera oportunidad es más grande con este tipo de unidades que las de tipo pluma, pero el código debe estar alineado apropiadamente y colocado cerca del borde de la tarjeta o documento.

Los ***lectores tipo rastrillo o CCD*** usan un dispositivo similar al encontrado en las cámaras de video. Para utilizar estos equipos, se coloca el extremo que contiene la "boca" o ventana de lectura sobre el código, el cual es iluminado por el CCD. La reflexión de esta luz se mide después en los foto-sensores del lector. Por lo tanto, se requiere hacer contacto físico con el código, pero a diferencia de los de tipo pluma no hay movimiento que degrade la imagen al tallarla.

Los ***lectores portátiles tipo pistola*** utilizan luz emitida por un diodo láser o un láser de Helio-Neón. Un espejo rotatorio u oscilatorio dentro del equipo mueve el haz de un lado a otro a través del código de barras, de modo que no se requiere movimiento por parte del operador. El lector puede estar alejado 2 a 20 cm del código, aunque actualmente existen algunos lectores especiales que pueden leer a una distancia de hasta 10 metros.

Los ***lectores láser fijos*** son básicamente lo mismo que el tipo anterior, pero montados en una base. La ventana de lectura se coloca frente al código a leer (generalmente se orientan hacia abajo) y la lectura se dispara al pasar el artículo que contiene el código frente al lector y activarse un sensor especial. Esta configuración se encuentra frecuentemente en bibliotecas ya que libera las manos del operador para que pueda pasar el libro frente al lector. También se utiliza en sistemas automáticos de fábricas y almacenes, donde el lector se coloca sobre una banda transportadora y lee el código de los artículos que pasan frente a él.

1.6 ¿Por qué una interfaz Web?

"La interfaz Web, tras su rápido despliegue en el mundo Internet, se ha revelado como paradigma de interfaz de usuario, gracias a sus características que la hacen ser amigable, intuitiva, independiente de arquitectura y con una curva de aprendizaje rápida. Es por ello por lo que está siendo utilizada actualmente por las casas de software como interfaz de sus servidores de aplicaciones (Microsoft Back Office, Lotus Domino, iPlanet Application Server, Oracle...), posibilitando una utilización óptima de los recursos software de una compañía. Esta tecnología suele estar basada en el uso de lenguajes como Java y mecanismos de comunicación distribuida tales como DCOM (Distributed Component Object Model, Modelo de Objetos de Componentes Distribuidos), CORBA (Common Object Request Broker Architecture, Arquitectura Común de Intermediarios de Peticiones de Objetos),RMI (Remote Method Invocation, Invocación de Métodos Remotos) o SOAP (Simple Object Adapter Protocol, Protocolo Simple de Adaptadores de Objetos), que posibilitan que el usuario interactúe, mediante clientes ligeros o páginas generadas dinámicamente, con servidores distribuidos de forma que se aprovechen los recursos eficientemente."[4]

A continuación se comentarán algunas de las herramientas de programación que fueron utilizadas para la implementación del Sistema.

1.7 Herramientas y Entorno de Programación

En este tópico se hará referencia a algunas de las herramientas que serán utilizadas durante el proceso de desarrollo de software de la aplicación Control de Acceso de la UCI, el Proceso Unificado de Desarrollo (RUP) utilizando el Lenguaje Unificado de Modelado (UML), el Visual Studio .NET como entorno y a la vez de ella se tomo el C# como lenguaje de programación.

Las herramientas de programación elegidas fueron:

- ✓ Metodología Proceso Unificado de Desarrollo (RUP)
- ✓ Microsoft Visual Studio .NET
- ✓ Microsoft SQL Server 2000

Serán expuestas algunas de las razones para apoyar esta elección.

1.7.1 El Proceso Unificado de Desarrollo

El Proceso Unificado de Desarrollo RUP es un proceso de desarrollo de software donde durante el paso por las diferentes etapas de desarrollo se van a "transformar los requerimientos de los usuarios en un sistema software" [4]. Está basado en componentes. Utiliza el Lenguaje Unificado de Modelado (UML) para "diseñar" los esquemas (diagramas) de un software. También está dirigido por casos de uso, está centrado en la arquitectura y es iterativo e incremental.

Esto hace que esta metodología que aunque nueva se nutre y mejora de otras ya existentes, lo que hace RUP es unificar, y valga la redundancia, estas tecnologías existentes pero que se han quedado un poco cortas a la hora de diferentes factores en el desarrollo de software.

1.7.2 ¿Por qué Visual Studio .NET?

Framework. NET es una plataforma confiable y madura, el Visual Studio .NET ofrece muchas más ventajas, comodidades, más estabilidad y rentabilidad que muchas otras con mucho más tiempo en el mercado.

Algunas características del Framework .NET:

- Es un conjunto de tecnologías que Microsoft ha integrado en una única plataforma con el objetivo de facilitar el desarrollo de este nuevo tipo de servicios de tercera generación.
- Mejora el rendimiento de aplicaciones Web típicas. ASP.NET incluye características de compilación y almacenamiento en caché avanzadas que

mejoran el rendimiento dos o tres veces por encima de la aplicaciones Active Server Pages (ASP) existentes.

- Permite a los desarrolladores utilizar cualquier lenguaje de programación e integrar aplicaciones escritas en diferentes lenguajes, lo que permite mejorar sus conocimientos actuales de desarrollo sin necesidad de nueva formación.
- Servicios Web XML: pequeñas aplicaciones reutilizables escritas en el lenguaje universal XML que permiten comunicar datos a través de Internet, entre fuentes interconectadas proporcionando una interfaz común entre aplicaciones existentes en servidores independientes, pueden obtener información de los Servicios Web publicados por los servidores.

1.7.3 ¿Por qué Microsoft SQL Server 2000 como servidor de base de datos?

Es un potente Servidor de Base de Datos y magnifica herramienta de Análisis de la información. Proporciona la seguridad, fiabilidad y escalabilidad necesarias para poner en marcha cualquier aplicación en el menor tiempo posible, destacándose en sus sencillas tareas de administración. Destacar que el SQL Server 2000 ostenta marcas de referencia en cuanto a escalabilidad y confiabilidad, que son críticas para el éxito de una base de datos empresarial. Tanto si lo que se mide es la velocidad en el desarrollo de aplicaciones como la velocidad del procesamiento de transacciones

1.7.4 Rendimiento y Escalabilidad

El rendimiento es uno de los temas más controvertidos a la hora de comparar el Visual Studio.NET con otra plataforma porque cuando independientemente de los resultados que muestren unos u otros defendiendo una plataforma, la otra parte nunca parece dispuesta a aceptarlos alegando disparidad de criterios como el hardware empleado, distintos tipos de optimizaciones utilizadas, etc.

La escalabilidad es la capacidad de un sistema de incrementar sus prestaciones en función del número de usuarios simultáneos que lo utilizan. El Visual Studio .NET ofrece métodos para la escalabilidad como la carga balanceada que permite a un cluster de servidores colaborar y dar un servicio de forma simultánea.

1.8 La solución

La UCI, donde será implementado el sistema de Control de Acceso tiene una arquitectura que permite este tipo de interfaz Web y a los sistemas que se necesita acceder también nos brindan ese servicio por lo que se implementará un sistema a la mediada que sea muy bien pensado, diseñado y adaptable al entorno, atendiendo a todos los requerimientos y a las funcionamiento de la Universidad.

Existen muchos sistemas de Control de Acceso en el mundo, con muchos años de experiencia incluso, que pudieron comprarse, pero la Universidad estaría incurriendo en un gasto innecesario ya que aquí se cuenta con capital humano suficiente como para llevar a cabo una tarea como esta y tal vez este sea el aporte económico más relevante que hizo el sistema: no gastar recursos monetarios en él, quizás en un futuro en otra organización donde se pueda implantar un sistema como este, se pueda comercializar el sistema de Control de Acceso y entonces la Universidad sí percibiría un aporte real.

CAPITULO II

CARACTERÍSTICAS DEL SISTEMA

2.1 Introducción

El Capítulo 2: Características del Sistema, se basa en el Proceso Unificado de Desarrollo (RUP) y el Lenguaje Unificado de Modelación (UML) y son explicadas paso a paso las características y funcionalidades del Sistema de Control de Acceso a la UCI.

El Proceso Unificado esta dirigido por casos de usos, centrado en la arquitectura y es iterativo e incremental. El desarrollo de este capítulo es muy importante porque es donde los desarrolladores, los usuarios u clientes finales proponen una vista común de cómo funciona y como debería funcionar el software de ya existir, los requerimientos funcionales que son capaces de lograr en esta parte del proceso de desarrollo del software evitará, que la fase de implementación y prueba se alargue más, que los desarrolladores y programadores no entiendan el funcionamiento del negocio ahora en esta parte y cuales son sus objetivos y las metas que se quieren lograr con el software.

En fin, en este capítulo, se analizarán los requerimientos del software que desembocarán en casos de uso, diagrama de actividades y modelos de casos de uso, modelo de objetos y el diagrama de casos de uso del sistema que estos describen la funcionalidad del sistema.

2.1 Situación Problémica

La Universidad de Ciencias Informáticas (UCI) por sus características especiales la hacen un objetivo estratégico para el desarrollo de las Ciencias Informáticas en el país. La Universidad de Ciencias Informáticas (UCI) necesita tomar medidas para controlar la entrada y salida del personal a sus instalaciones, con el objetivo de proteger los medios con que cuenta la institución por lo que se hace necesaria la vigilancia continua y estudios de comportamiento de las personas que entran y salen de la UCI.

A pesar de no contar con un sistema que deje constancia de los horarios de entrada y salida de la misma, ya cuenta con un Sistema de Acreditación donde se encuentran todos los datos de las personas relacionadas con la UCI, no cuenta con ninguna aplicación que valide si la persona está autorizada a entrar/salir de la misma, ni que registre las horas en la que estos eventos han ocurrido, ni se cuenta con un historial de estos para su posterior procesamiento, ya sea para un fin estadístico, para conocer las horas trabajadas por un profesor o trabajador, la personas que se encuentran dentro o fuera y a que hora lo hicieron. Esa información que se irá almacenando puede contener varios datos de interés. Todas las personas relacionadas de alguna manera con la UCI poseen un carnet de identificación o solapín, con este carnet que tiene impreso algunos datos de las personas y un código de barras de clave única.

2.2 Objeto de Automatización

El Departamento de Seguridad y Protección Física ha tomado la decisión de implementar un sistema para el Control de Acceso a la UCI que controle y registre los horarios de la entrada/salida de las personas a sus instalaciones, que posibilite detectar posibles violaciones de la seguridad y/o la posible entrada de personas ajenas al centro y registre la fecha y la hora en que estos incidentes se producen estas acciones y por quien, hacer búsquedas de los datos que se quieran conocer de la personas, las personas que más entran/salen de la UCI, las cantidades por tipo de solapín, es decir, la cantidad de estudiantes, de trabajadores, de profesores, de mercerizados; en fin, se

pretende con este sistema de Control de Acceso conocer datos actualizados de lo relacionado con el acceso a la UCI.

El Sistema de Control de Acceso pretende automatizar los siguientes procesos:

- Identificación del Personal.
  - Reconocer la Persona al captar los datos del carnet de Identificación de las Personas en los puntos de acceso.
  - Denegar el acceso o no al centro.
  - Para el caso de los visitantes chequear en el Sistema de Control de Visitantes si las personas ya han sido autorizadas a entrar al centro.
  - Maneja anti-pass back

- Registrar Horarios
  - Registrar horario en el que las personas autorizadas entran/salen de la UCI

- Reportes
  - Reportar incidencias de las entradas/salidas de personas y en que horario se realizan.
  - Reporte por fechas de las entradas/salidas
  - Búsqueda de los principales indicadores.
  - Detectar personas que más salieron/entraron de la UCI
  - Reportes de los horarios de entrada/salida de una persona.

2.3 Sistema Propuesto

Como ya habíamos comentado antes, la UCI cuenta con un Sistema de Acreditación donde se encuentran todos los datos de las personas relacionadas con la UCI y para llegar a ellos los sistemas comúnmente lo hacen mediante la comparación de los códigos de barras almacenados por este sistema de Identificación y comparándolos con la lectura que se hará de los códigos de barras impreso en los carnets de identificación con un lector de código de barras.

Estos códigos son de clave única a los respectivos datos de los propietarios de los carnets que están almacenados en el sistema de Identificación de la UCI y tendremos que comprobar si existen o no y de existir si están en activo

De existir el código de barras o el número del solapín en el sistema de Identificación puede suceder lo siguiente:

- Si carnet esté en activo (activado), este término indica que el carnet no ha sido "desactivado" en el sistema, algunas causas de la desactivación son: pérdida, baja del centro, o la expiración del tiempo que inicialmente le fue asignado a este carnet. Si no, entonces se deniega el acceso y se informa de la situación.
- Son mostrados los datos del resultado de la comparación de la comparación del código leído con el del carnet: nombre, apellidos, y otros, incluida la foto del propietario del carnet en cuestión, de esta forma, el agente tendrá un medio más para poder comprobar que la persona que le está mostrando el carnet es el verdadero propietario del mismo.

Todavía no puede registrarse el horario del evento que ha ocurrido, es necesario realizar otra validación, tal vez la más importante de todas y se basa en lo siguiente, una persona que ya haya entrado no puede volver a registrarse como entrada hasta no salir del sistema y viceversa, a esto se le llama, anti-pass back.

Habiendo hecho esta importante validación, entonces se registra el horario en que dicha personas está entrando/saliendo de la UCI.

De no suceder ninguno de los eventos anteriores, se notifica el acceso denegado a esta persona, es decir, cuando el carnet está desactivado u ocurre un anti-pass back, también guardamos los datos de la persona y el horario en que se denegó el acceso para que quede constancia de ocurrido y que luego pueda ser procesada esta información de accesos denegados.

El operador del sistema podrá auxiliarse mediante algunos reportes para informar a las personas que lo requieran y cuando lo requieran.

Este sistema formará parte de toda una estructura organizativa para la gestión interna de la Universidad.

Con el objetivo de lograr la interacción que se quiere entre las aplicaciones en la UCI y alcanzar una alto grado de informatización, el sistema de Control de Acceso surtirá con sus datos al sistema de Asistencia que detectará las llegadas tardes y el ausentismo, y detectar si una persona se encuentra dentro de la Universidad o no haciendo uso de las horas de entrada y salida de los trabajadores.

2.4 Sistemas de Control de Acceso Existentes

La Universidad cuenta con un sistema de Control de Entradas al Comedor. Este valida el código de barras del carnet contra el Sistema de Identificación y registra las entradas del personal.

Este sistema se ha utilizado como referencia para la implementación del Sistema de Control de Acceso porque ya cuenta con algún tiempo de implementado y con muy buen desempeño, existen 3 comedores con 2 puertas de entrada cada uno, y diariamente, son almacenados alrededor de 15 000 registros en su base de datos.

Existen muchos sistemas de Control de acceso, pero en la Universidad es necesario un sistema que se corresponda a los requerimientos del sistema en si y a las condiciones de la Universidad en cuestiones de organización, funcionamiento y seguridad;

independientemente a esto este sistema de Control de Acceso tributará información al Sistema de Asistencia con los horarios de entrada y salida del personal a la Universidad.

2.5 Objetivos

El objetivo general de este proyecto es automatizar el Control de Acceso a la UCI para poder controlar el flujo de entrada/salida de personas, determinar posibles violaciones de la seguridad, datos relacionados con los accesos y sus comportamientos en la UCI, esto ayudará al Dpto. de Seguridad y Protección Física en una eficiente gestión en sus funciones y poder determinar más adelante, entre otras cosas, estos horarios y poder controlar la asistencia del personal y por ende, las hora de permanencia y las trabajadas de manera instantánea así como posibles violaciones de la seguridad.

Los objetivos específicos son:

- Manejar usuarios del sistema en dependencia de su nivel de acceso.
- Controlar la entrada/salida de personas a la UCI
- Reconocer a una persona y registrar los momentos de entrada/salida
- Manejar el anti-pass back
- Detectar posibles intrusos o violaciones
- Reportar principales incidencias de personas que más entraron y(o) salieron en un tiempo definido
- Reportar datos de la entrada/salida por personas (si es necesario)
- Hacer búsquedas de personas (si están dentro o fuera de la UCI)

2.6 Descripción del Negocio Actual

El Control de Acceso a las instalaciones de la UCI que se realiza en los puntos de acceso lo realiza un Agente de Seguridad y Protección (AGESP) sólo mirando si la persona es portadora de un carnet de identificación o no. Esto traer consigo que pueda entrar personas ajenas al centro sin chequear correctamente la validez del carnet o si este está en activo, o simplemente portando otro carnet que no es el suyo. Para el

acceso de los visitantes, diariamente emiten un documento con la relación de los visitantes autorizados a entrar y quien los autoriza. En caso de que estos visitantes lleguen de improviso entonces, se trata de localizar a esta persona por teléfono para que los autorice a entrar.

2.7 Descripción del Negocio Propuesto

La Universidad de Ciencias Informáticas (UCI) necesita tomar medidas para controlar la entrada y salida de la misma. Tiene implementado un sistema de identificación mediante un carnet que posee lo datos de cada persona y lleva impreso un código de barra que permite acceder a los servicios del centro. El sistema de Comedor, es uno de estos servicios, que ya está en funcionamiento y controla la entrada del personal a los comedores, y se tienen previstos otros que ya están en fase de desarrollo. Todos estos sistemas que utilizan esta forma de identificarse contra el Sistema de Acreditación de la UCI.

El Control de Acceso a la UCI actualmente se realiza en los puntos de entrada y salida de la Universidad por Agentes de Seguridad y Protección (AGESP) si es una persona que le muestra un carnet de identificación y esta persona entra a la Universidad, en caso de los estudiantes para salir, sólo pueden salir en los horarios específicos de pase o por algún otro motivo, por ejemplo, pase por turno médico u temporal. Este simple chequeo puede que no es tan eficiente y puedan entrar elementos ajenos a la institución.

La entrada y salidas de las personas UCI pueden ser personales o masivas. Las personales se explican por si sola, las masivas se harán mediante unos dispositivos portátiles encargados de la lectura y almacenamiento de los códigos de barras para aliviar la demora del proceso de entrar/salir, por ejemplo, el transporte de profesores o trabajadores tienen que chequear entrada o salida, y es un poco lento a la hora de realizar el chequeo que cada uno de los mismos tengan que bajar y subir al transporte a chequear su entrada/salida.

Se pretende implementar un sistema de Control de Acceso donde serán automatizados los procesos de identificación del personal siguientes:

- Controlar la entrada/salida de personas a la UCI
- Reconocer a una persona y registrar los momentos de entrada/salida
- Manejar el anti-pass back
- Detectar posibles intrusos o violaciones
- Reportar principales incidencias de personas que más entraron /salieron en un tiempo definido
- Reportar datos de la entrada/salida por personas (si es necesario)
- Hacer búsquedas en los reportes de personas (si están dentro o fuera de la UCI)
- Manejar usuarios del sistema en dependencia de su nivel de acceso.

Evidentemente en materia de seguridad la institución podrá quedar más segura en cuanto al acceso con una la adecuada gestión del Sistema de Acreditación que es básicamente a donde el Sistema de Control de Acceso accederá para hacer las peticiones sobre las identidades de las personas y al Sistema de Control de Visitantes que brindará los datos de los visitantes y el estado de los mismos, si ya está aprobado su acceso o no, para controlar y registrar la entrada/salida de los mismo al centro.

Algunos beneficios que garantizará las funcionalidades del un sistema Control de Acceso:

- Eliminación de tarjeta de firmas o el reloj chequeador y el trabajo manual asociado al procesamiento de los horarios trabajados o de permanencia.
- Detección inmediata de Ausentismo y Retardos.
- Cálculo de tiempo trabajado; ordinario y extra.
- Disponibilidad de reportes con información actualizada al último minuto.
- Eliminación de la demora en los puntos de acceso.

Otro sistema que debemos tener muy en cuenta es el de Control de Visitantes, tendremos que chequear si la personas cuando son ajenas al centro y ya ha sido

autorizada su entrada, por lo tanto tenemos que manejar los horarios en que estas personas hicieron entrada y salida a las instalaciones de la UCI.

Las entradas y salidas pueden ser personales o masivas. Al entrar o salir, así de forma masiva los Agentes de Seguridad contarán con dispositivos portátiles y recolectan todos los códigos de barras de las personas, luego se "descargarían" estos en un formulario especial para estos fines todos estos datos serán insertados en la base de datos y luego mecanismos en el servidor se encargarán de distribuir esta información ya sea de salida o de entrada para sus respectivas tablas.

2.7 Actores y Trabajadores del Negocio

ACTORES DEL NEGOCIO	JUSTIFICACIÓN
Personas	Cualquier persona (estudiante, profesor, trabajador, mercerizados) o un visitante previo autorizado o no) que solicite el acceso a las instalaciones de la UCI, presentando su identificación en los puntos de entrada/salida.

TRABAJADORES DEL NEGOCIO	JUSTIFICACIÓN
Agentes de Seguridad (AGESP)	El Agente de Seguridad de servicio en el punto de control de acceso, chequeando que las personas muestren su identificación y no haya violaciones en lo relacionado con el acceso.
Ejecutivos	El personal del Dpto. de Seguridad y Protección Física y otros que están autorizados tratar con este tipo de información.

2.7.1 Descripción de los Casos de Uso del Modelo del Negocio

Los casos de uso le proporcionan a los analistas del sistema un medio intuitivo para capturar los requisitos funcionales para cada usuario o sistema externo. Estos le permiten a los desarrolladores y a los clientes lleguen a tener una visión común sobre el problema en sí y que es lo que realmente necesitan la empresa y los clientes.

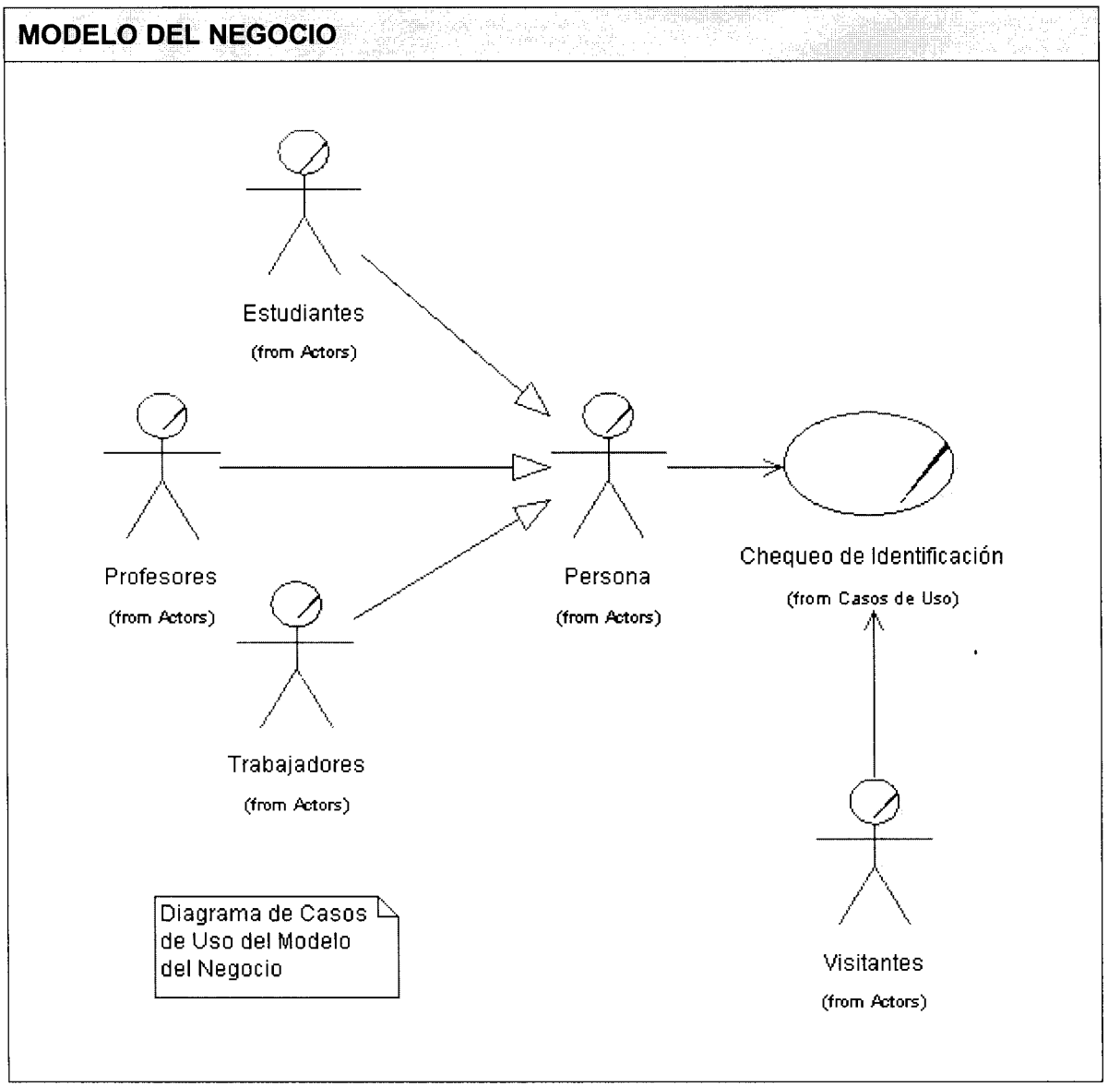
CASOS DE USO DEL MODELO DEL NEGOCIO

- ✓ Chequeo de Identificación (CU-1)

CU-1	
CHEQUEO DE IDENTIFICACION	
Actores	Persona
Propósito	Se requiere que las personas presenten su identificación para entrar/salir de la UCI en el punto de control de acceso al Agente de Seguridad
Resumen : El caso de uso inicia cuando una persona para entrar/salir de la UCI se identificarse, para eso muestra su carnet de Identificación. Si posee su identificación se autoriza el acceso a esta persona, si no, no se autoriza. Los visitantes tienen que esperar por la autorización.	
Referencias: -	
Acción del actor	**Respuesta del Proceso de Negocio**
1 La persona requiere ***entrar/salir*** a la UCI	**2** El Agente le solicita a la persona que se identifique, si no presenta o no posee identificación, ir al paso **8** **3** Si la identificación UCI no es válida, ir al paso **8** **4** Si la identificación de la persona es válida, entonces ir al paso **6**

	5 Si es un visitante, el Agente comprueba que los datos de esta persona existan en la lista de visitantes autorizados **5.1** Si no están en la lista de autorizados entonces, ir al paso **7** **5.2** Si existen, se le toman los datos, y le proporcionan una identificación temporal (carnet este que a la salida tiene que devolver) de visitante. Ir al paso **6** **5.3** Si el visitante está saliendo de la UCI, ir al paso **10**
	6 El Agente de Seguridad le notifica a la persona el Acceso Concedido, ir al paso **7**
7 La persona puede entrar a la UCI	
	8 El Agente de Seguridad le notifica a la persona el Acceso Denegado, ir al paso **9**
9 La persona NO puede entrar a la UCI.	
10 En caso que, la salida de un visitante este entrega la identificación temporal que le fue asignada y sale de la UCI	
	11 El agente recibe la identificación temporal.
Prioridad: Alta (Este proceso define o no la entrada/salida de la UCI)	
Mejoras: Cuando el proceso sea automatizado, el agente podrá tener otra manera de comprobar si la identificación es de una persona UCI y si está activada o no. En el caso que una persona desee visitar a una persona UCI, mediante el servicio Web del sistema de Visitantes es posible determinar está autorizada o no y si dicha la persona solicitada se encuentra en la Universidad o no.	

2.7.2 Diagrama de Casos de Uso del Modelo del Negocio

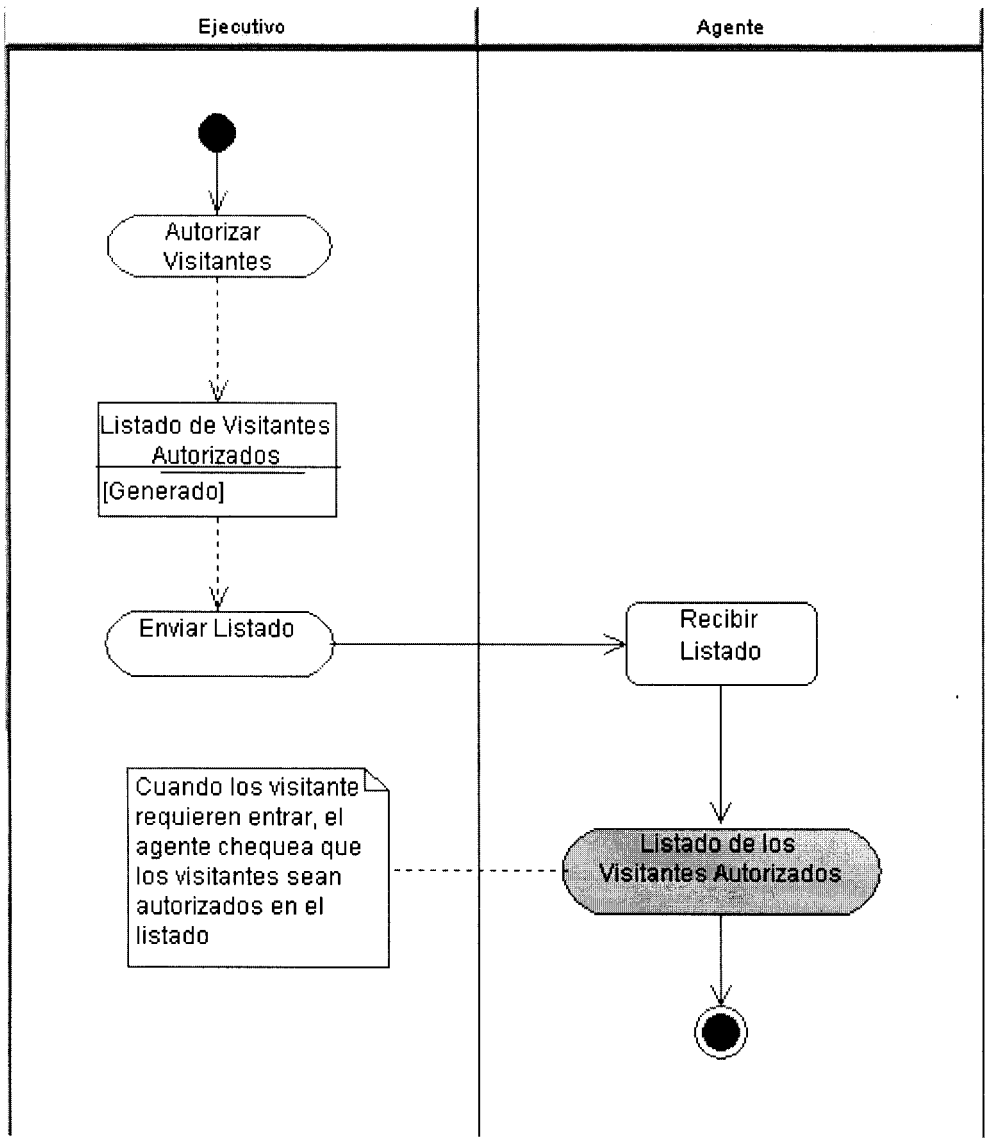


2.7.3 Diagramas de Actividades

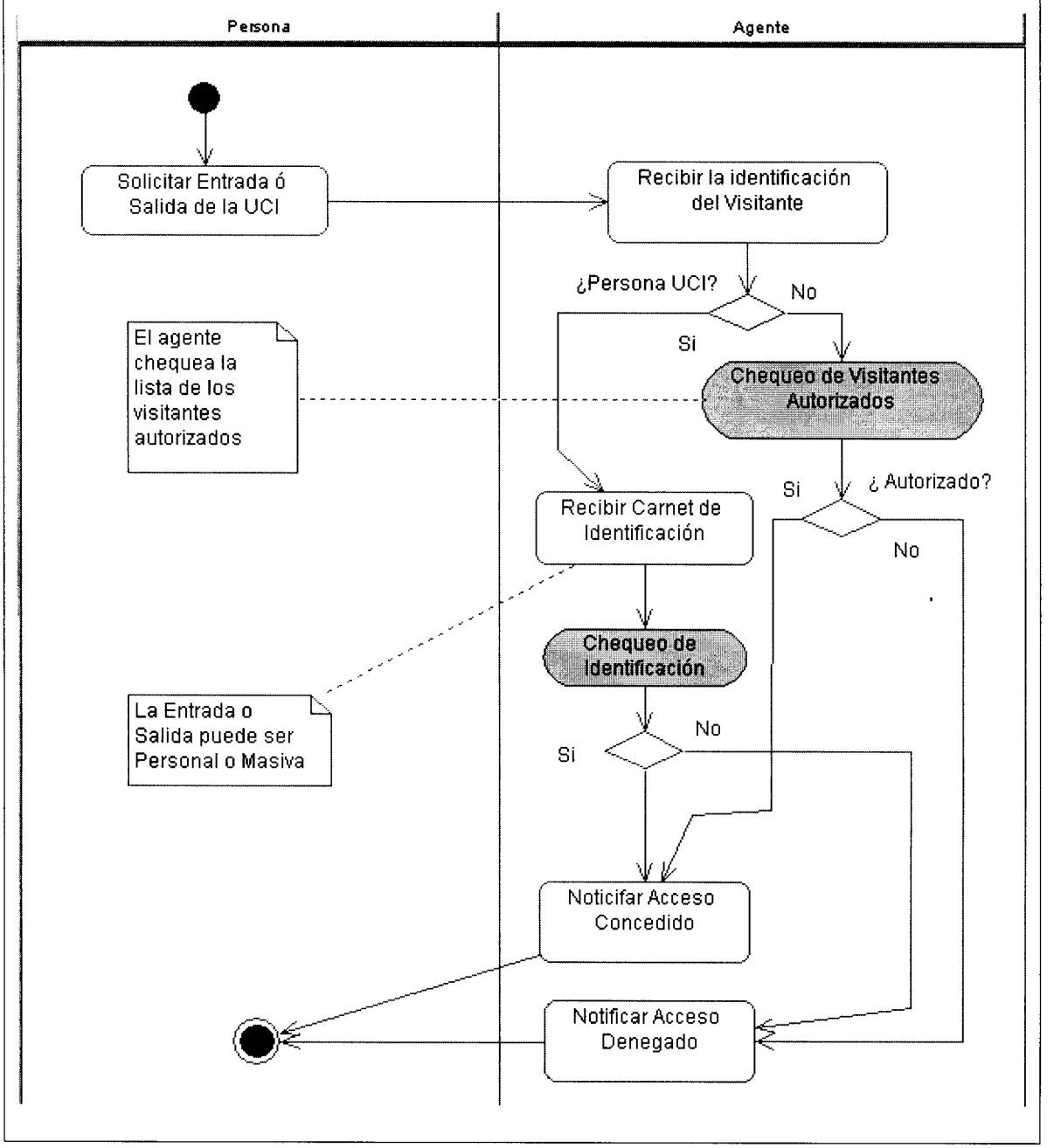
Los diagramas de actividades ayudan a describir el proceso que ocurre en el proceso del negocio y las interacciones que existen entre los trabajadores del negocio que serán los futuros actores del sistema.

Los dos diagramas de actividades a continuación representan, el primero, el proceso de la conformación del listado de los visitante por parte de los responsables de esta tarea (Ejecutivos) y el segundo representa el proceso del chequeo de identificación como tan, donde se tiene en cuenta si la persona es un visitante para buscarlo en dicho listado. El la descripción se detallará aún más sobre este proceso.

LISTADO DE VISITANTES

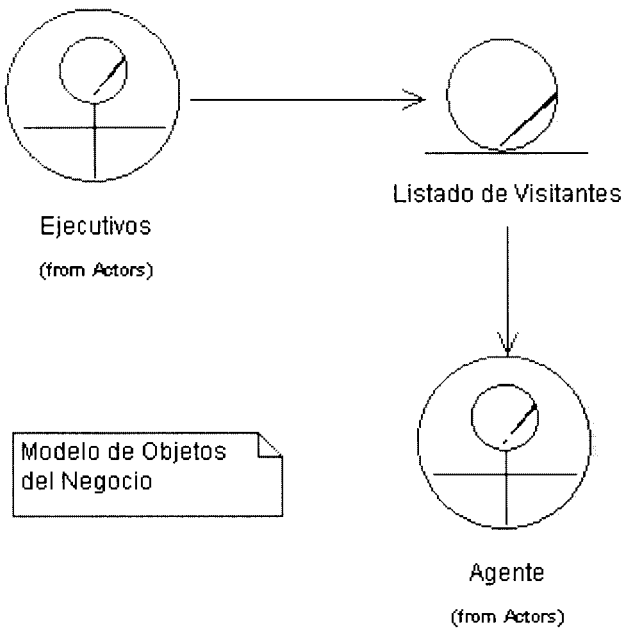


CHEQUEO DE IDENTIFICACION



2.7.4 Diagrama de Clases del Modelo de Objetos

DIAGRAMA DE CLASES DEL MODELO DE OBJETOS



2.8 Especificación de los Requisitos del Software

"El propósito fundamental del flujo de trabajo de los requisitos es guiar el desarrollo hacia el sistema correcto. Esto se consigue mediante una descripción de los requisitos del sistema (es decir, las condiciones o capacidades que le sistema debe cumplir) suficientemente buena como para que pueda llegarse a un acuerdo entre el cliente (incluyendo los usuarios) y los desarrolladores sobre qué debe y que no debe hacer el sistema."[1]

El sistema de Control de Acceso controlará la entrada/salida de las Personas UCI (estudiantes, profesores y trabajadores) y de los visitantes, los datos de los visitantes los almacena el Sistema de Control de Visitantes, para eso deberá llevar el control de los respectivos horarios de entrada y salida de todas estas personas al centro.

2.8.1 Dependencias y Relaciones

Para chequear si la persona que entra/sale por los puntos de acceso es una Persona UCI, nuestro sistema se apoyará en los datos que brinda el servicio Web que el Sistema de Acreditación existente en el que se apoyaría el sistema para reconocer y validar la autentificación de las personas que acceden a la Universidad.

También el Sistema de Control usará el servicio Web que brinda el Sistema de Control de Visitantes, ya que los visitantes previstos e imprevistos necesitan registrar sus datos en dicho sistemas y ser autorizados para poder entrar a la UCI.

2.8.2 Requerimientos del Sistema

1. Controlar la entrada/salida de personas a la UCI
2. Consultar el Sistema de Acreditación de las UCI y reconocer la persona.
3. Registrar los horarios de entrada/salida
4. Hacer búsquedas de las personas (si están dentro o fuera de la UCI)
5. Manejar el Anti-pass back
6. Detectar posibles intrusos o violaciones
7. Reportar principales incidencias de las entradas/salidas de las personas en un tiempo definido
8. Reportar datos de la entrada/salida por personas
9. Consultar Sistema de Control de Visitantes

2.8.3 Casos de Uso del Sistema

1. Chequeo de identificación
2. Chequeo de Personas
3. Registrar Horarios
4. Chequeo de Visitantes
5. Gestionar Información

2.9 Definición de los Actores de Sistema

ACTORES	JUSTIFICACION
Personas	Cualquier persona (estudiante, profesor o trabajador o visitante previo autorizado o no) que solicite el acceso a las instalaciones de la UCI, presentando su identificación en los puntos de entrada/salida.
Ejecutivos	Departamento de Seguridad y Protección Física que están interesados en saber la información que brinda el sistema (reportes) para estar informados de las principales incidencias.
Agentes de Seguridad (AGESP)	Agentes de Seguridad en servicio en el punto de control de acceso, chequeando que las personas muestren su identificación y no haya violaciones en lo relacionado con el acceso.
Sistema de Acreditación (UCI Personas)	Sistema que contiene la información de todas las personas de la UCI. El Sistema de Control de Acceso interactúa con su Servicio Web para acceder a estos datos.
Sistema de Control de Visitantes (UCI Visitas)	Sistema que controla todo el proceso y contiene los datos de los visitantes. El Sistema de Control de Acceso interactúa con su Servicio Web para acceder a sus datos.

2.9.1 Descripción textual de los Casos de Uso del Sistema

CU-1	
CHEQUEO DE IDENTIFICACION	
Actores	Agente(Inicia), Persona
Descripción : El caso de Uso se inicia cuando el agente le pide la identificación de la persona que requiere entrar/salir de la UCI, chequea que no haya anti-passback.	
Referencias:	R1 y R6 Casos de Uso asociados: • Chequeo de Personas (include) • Registro de Horarios (include) • Chequeo de Visitantes (extended)
Precondiciones:	Todas las personas UCI, poseen un carnet con algunos de sus datos, un número de solapín y un código de barras.
Poscondiciones:	Luego de que se ejecuten los casos de uso de realización que tiene incluido queda registrado el horario de la acción que se llevó a cabo; entrada, salida o acceso denegado.

CU-2	
CHEQUEO DE PERSONAS	
Actores	Agente, UCI Persona
Descripción : El caso de Uso es de realización (include), el código de barras del carnet o el número de solapín es comparado con los datos almacenados en UCI Persona. Deben existir y estar activos para tener acceso y devuelve los datos de esta persona.	
Referencias:	R-1, R-2, R-5 y R-6
Precondiciones:	Con el código de barras del carnet o el número de solapín es posible identificar a las personas utilizando el servicio Web del Sistema de Identificación.
Poscondiciones:	Devuelve los datos de la persona si existen y está activado el

	código de barras o el solapín.

CU-3	
REGISTRAR HORARIOS	
Actores	Agente
Descripción : El caso de Uso es de realización (include) se inicia después de haberse ejecutado el **CU-2** o el **CU-4** en dependencia de quien esté siendo procesado (persona UCI o visitante). Registra los horarios de entrada, salida o accesos denegados de las personas.	
Referencias:	R-1 y R-3
Precondiciones:	Los datos de la persona que entra/sale fueron validados contra UCI Persona ó UCI Visitas.
Poscondiciones:	Los datos de esta persona quedarán registrados junto a la fecha, la hora y la acción (entrada, salida o denegados)

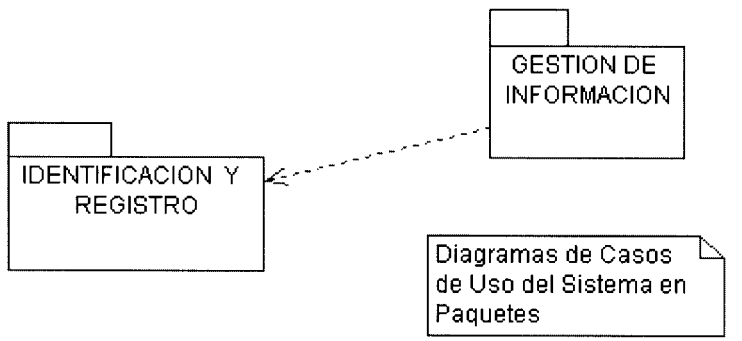
CU-4	
CHEQUEO DE VISITANTES	
Actores	Agente, UCI Visitas
Descripción : El caso de Uso es de realización (exclude) se inicia sólo cuando la persona que requiere entrar/salir de la UCI es un visitante el servicio Web de Sistema de Control de Visitantes (UCI Visitas). Se chequea que este carnet temporal esté autorizado.	
Referencias:	R-1, R-3, R-5, R-6 y R-9
Precondiciones:	Al visitante le asignan una identificación temporal que sólo cuenta con un número de solapín.
Poscondiciones:	Notificar que el visitante está autorizado a entrar o si no puede entrar por no estar autorizado porque no lo encuentra o en el caso que sea un visitante previsto no ha sido aprobada su solicitud.
Requerimientos Especiales: Se ejecuta sólo sí se especifica que la persona es un visitante.	

CU-5	
GESTIONAR INFORMACION	
Actores	Agente (Inicia), Ejecutivo
Descripción : El caso de Uso se inicia el Agente cuando necesita para su gestión datos relacionados con el acceso o necesita saber si alguna persona esta ausente o ya entró a la UCI. El Ejecutivo puede acceder también a la información. Reporte de cantidades de entradas, salidas, accesos denegados, por fecha, rangos de fecha, por tipo.	
Referencias:	R-2, R-4, R-6, R-7, R-8 y R-9
Precondiciones:	Sólo los ejecutivos autorizados y los agentes pueden acceder a esta información.
Poscondiciones:	Obtienen la información que necesitan

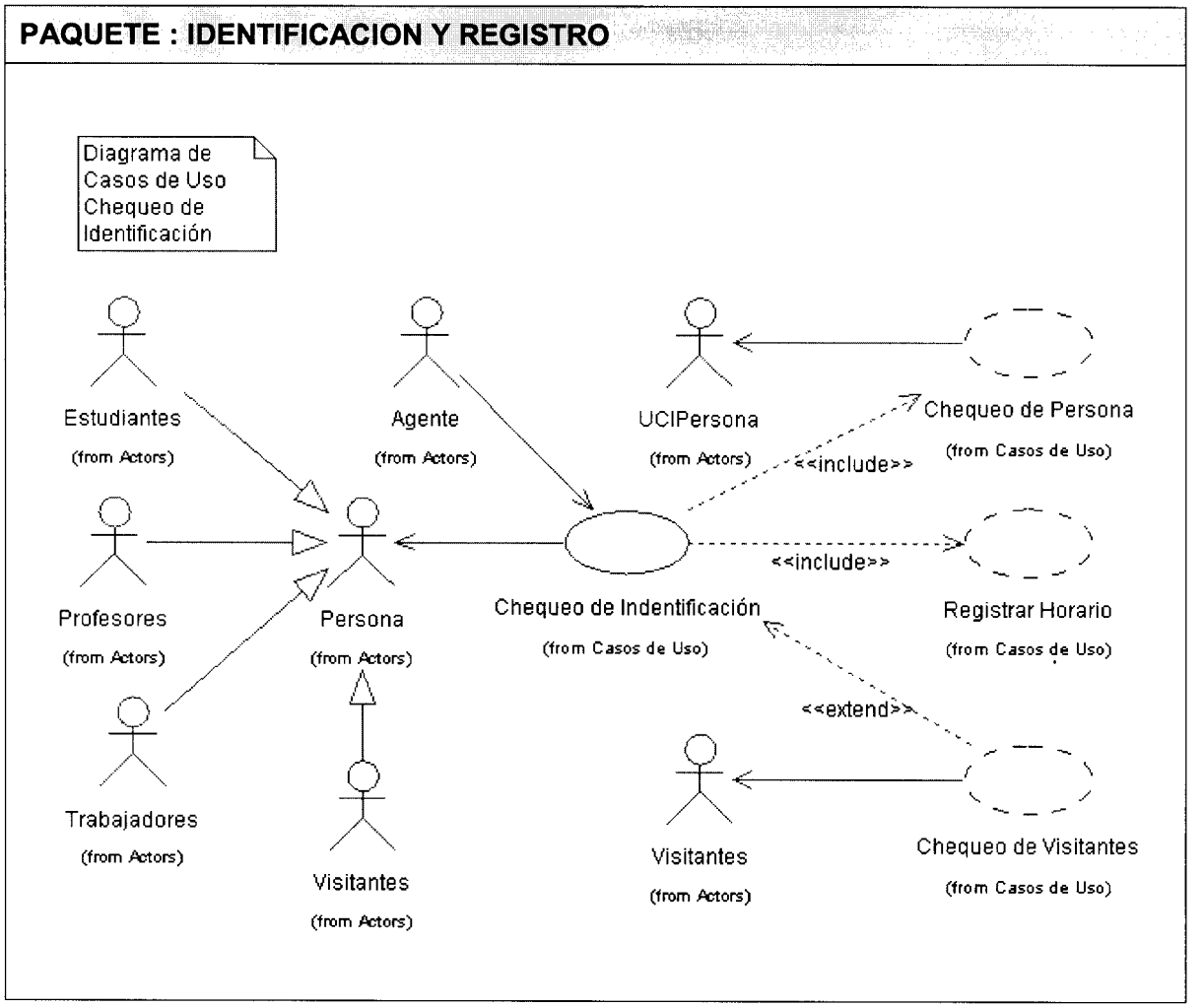
2.9.2 Diagrama de Casos de Uso por Paquetes

Para que se entiendan mejor y por su funcionalidad se han separados los casos de uso por paquetes.

DIAGRAMA DE CASOS DE USO EN PAQUETES



2.9.3 Paquete: Identificación y Registro



2.9.4 Paquete: Gestionar Información

PAQUETE: GESTIONAR INFORMACIÓN

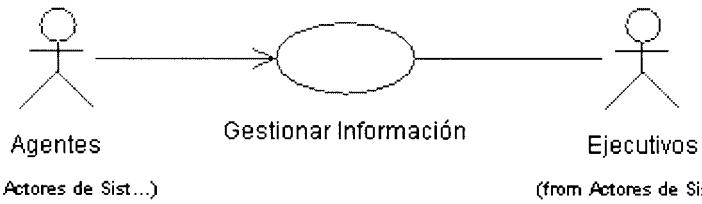


Diagrama de Casos de Uso
: Gestionar Información

2.10 Casos de Uso por Ciclos de Desarrollo

Debido a la necesidad y la premura de implementar en la UCI el Sistema de Control de Acceso para regular y controlar de forma automatizada las entradas/salidas. El sistema se desarrollará en un inicio los dos primeros ciclos y posteriormente se le irán ampliando las funcionalidades y posibilidades al sistema.

La seguridad en este caso pasaría a un tercer ciclo y no se desarrollará ahora en la etapa inicial puesto que se puede restringir acceso al sistema mediante políticas de seguridad en el servidor para las personas no autorizadas a usar el sistema. Sólo tendrán acceso los equipos de los puntos acceso a la UCI.

CICLO	CASOS DE USO	PAQUETE	JUSTIFICACION
1	✓ Chequeo de Identificación ✓ Chequeo de Personas ✓ Chequeo de Visitantes ✓ Registrar Horarios	Identificación y Registro	Este es el núcleo del sistema, los casos de uso incluido aquí caracterizan al sistema.
2	✓ Gestionar Información	Gestión de Información	Se reportan las principales incidencias ocurridas en la entrada, salida y denegados
3	✓ Seguridad	Seguridad	Debido a las características del sistema, la seguridad se puede tratar de una forma diferente.

2.11 Descripción de Casos de Uso expandidos

CASO DE USO	
CU-1	**CHEQUEO DE IDENTIFICACION**
Propósito	El agente chequea que la persona tenga una identificación "valida" y controla la ejecución del proceso de identificación.
Resumen: El caso de Uso se inicia cuando el agente le pide la identificación de la persona que requiere entrar/salir de la UCI, este comprueba si: ✓ dicho carnet no esté adulterado de cierta forma ✓ la persona posee una identificación válida de la UCI ✓ existen los datos de este carnet en el sistema de Identificación y que esté activado dicho carnet ✓ es visitante, chequea que su vista esté autorizada y registra la acción. Luego registra el horario de la acción	
Referencias	R1 y R6 Casos de Uso asociados: • Chequeo de Personas (include) • Registro de Horarios (include) • Chequeo de Visitantes (extended)

ACCION DEL ACTOR	**RESPUESTA DEL SISTEMA**
1. El usuario solicita al sistema registrar un acceso.	2. El sistema muestra la página para registrar el acceso.
3. El usuario introduce el código de barras del carnet o el número del solapín	4. Comprueba si existe el usuario y si está activado. Ver línea 3. 5. Si es un visitante chequea que el visitante ya ha sido autorizado. Ver línea 4 6. Registrar la fecha y el horario de la acción (entrada ó salida) si no hay anti-

8 .Notificar Acceso Denegado 9. Acceso Concedido	pass back. Ver sección 1 7. Si no se cumplen las líneas 3 y 5 ira a línea 8; sino ir a línea 9 y mostrar los datos de la persona.
PUNTOS DE EXTENSIÓN.	
Línea 3: Ver CU-2 Chequeo de Persona. Línea 4: Ver CU-4 Chequeo de Visitantes. Línea 5: Ver CU-3 Registro de Horarios	

CASO DE USO	
CU-2	**CHEQUEO DE PERSONAS**
Propósito	Chequea de la identificación es existe y está activada.
Resumen: El caso de Uso es de realización y es una funcionalidad del **CU-1**, accede a los servicios Web de UCI Persona para determinar si esta identificación existe y si esta activa, luego devuelve los datos de la persona en cuestión.	
Referencias	R2 y R6
ACCION DEL ACTOR	**RESPUESTA DEL SISTEMA**
1. Luego de introducidos los datos, el código o el núm solapín. 5 Devuelve los datos 6 Devuelve mensajes de que no existe	2. El sistema accede al Servicio Web de UCI Persona 3. Comprueba si existe el usuario y si está activado. 4. Si existe y está activado, ir a paso 5 4.1 Si no existe, ir al paso 6. 4.2 Si no está activado, ir al paso 7

7 Devuelve mensaje que no está activado	

CASO DE USO	
CU-3	**REGISTRO DE HORARIOS**
Propósito	Registrar el horario de las acciones (entrada, salida y denegados)
Resumen: El caso de Uso es de realización y es una funcionalidad más del **CU-1** registra los horarios de los accesos, entradas o salidas y en el caso de que exista anti-pass back entonces le registra el horario también.	
Referencias	R3, R6, R7

ACCION DEL ACTOR	**RESPUESTA DEL SISTEMA**
1. Luego de hacer los chequeos de identificación de personas y de visitantes.	2. Si es entrada, el sistema cheque que no haya anti-pass back y registra la entrada. 3. Si es salida, chequea que no haya una salida sin entrada (anti-pass back) y registra la salida. 4. Si hubo anti-pass, el sistema registra esta acción también la identificación dela persona
5. Devuelve el mensaje en cada caso.	

CASO DE USO	
CU-4	**CHEQUEO DE VISITANTES**
Propósito	Chequea si el visitante ya ha sido autorizado.
Resumen: El caso de Uso es de realización y es una funcionalidad más del **CU-1**, accede a los servicios Web de UCI Visitas para determinar si el visitante ya ha sido autorizado a entrar.	
Referencias	R1, R6 y R9

ACCION DEL ACTOR	RESPUESTA DEL SISTEMA
1. Luego de introducir el dato del visitante, el núm. Solapín	2. El sistema accede al Servicio Web de UCI Visita 3. Comprueba si ya el visitante ha sido autorizado a entrar, ir al paso 5. 4. Si no ha sido autorizado, ir al paso 6.
5. Devuelve los datos del visitante 6. Devuelve mensajes de que no ha sido autorizado a entrar.	

CASO DE USO	
CU-5	**GESTION DE INFORMACION**
Propósito	Consultar la información que proporcionará el sistema. Reportes de los accesos a la Universidad, estadísticas por día por mes, etc.
Resumen: El caso de Uso se inicia cuando un Agente necesita para su gestión datos relacionados con el acceso o necesita saber si alguna persona está ausente o ya entró a la UCI. El Ejecutivo puede acceder también a la información o el Agente le informa de la situación. Reporte de cantidades de entradas, salidas, accesos denegados, por fecha, rangos de fecha, por tipo, etc.	
Referencias	R1, R2, R4, R6, R7

ACCION DEL ACTOR	RESPUESTA DEL SISTEMA
1. El usuario (Agente ó Ejecutivo) selecciona del menú el tipo de reporte que quiere ver.	
	2. Se muestra el reporte seleccionado con los datos de la fecha actual
3. El usuario puede seleccionar otras fechas para visualizar los datos de ese reporte en dichas fechas.	
	4. Se muestra el reporte con los datos de la fecha seleccionada.
5. Así el usuario puede navegar por los reportes para consultar los datos de sus interés	

2.12 Conclusiones

Con la culminación de este capítulo ha quedado claras ya, las características que tendrá el sistema de Control de Acceso, quedaron bien detallados los casos de uso para poder entender los requerimientos y futuras funcionalidades del sistema, ahora sólo queda tratar de optimizar el modelo que se ha encontrado en las próximas iteraciones del proceso, pero no puede ser antes de pasar por los flujos de trabajo de análisis y diseño.

CAPITULO III

ANÁLISIS Y DISEÑO DEL SISTEMA

3.1 Introducción

En este Capítulo III, Análisis y Desarrollo se analizan los requisitos que fueron planteados en el capítulo anterior, Características del Sistema, para reestructurarlos y tener una visión más exacta de los requisitos tratando de mantener un poco la estructura del todo el sistema.

No es posible tener buenos resultados si no quedan bien formalizados los requerimientos funcionales del software, no se debe pasar a las etapas de implementación sin haber tenido éxito en esta etapa de análisis.

3.2 Diagramas de Clases de Análisis

DIAGRAMA DE CLASES DE ANALISIS: CHEQUEO DE IDENTIFICACION

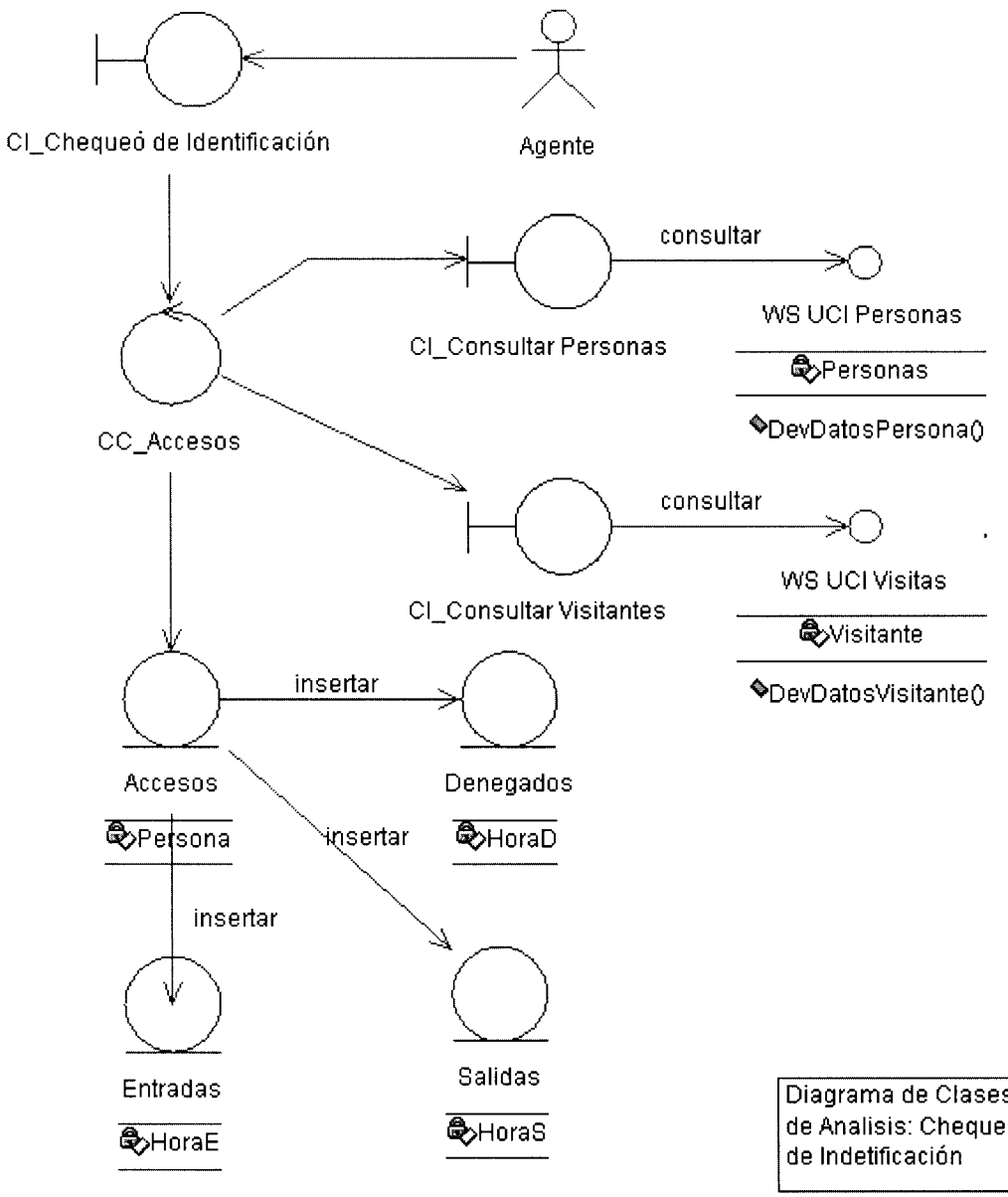
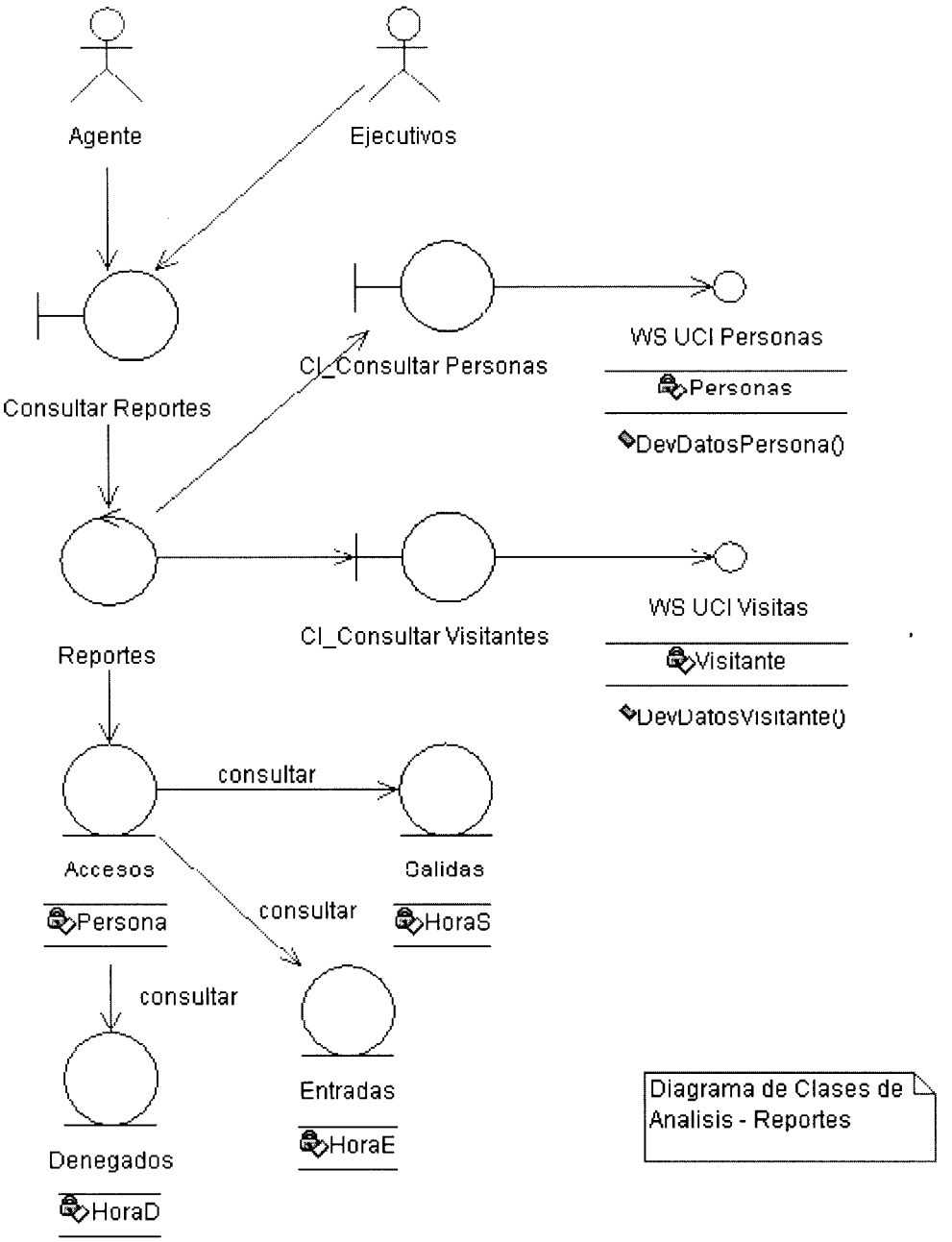


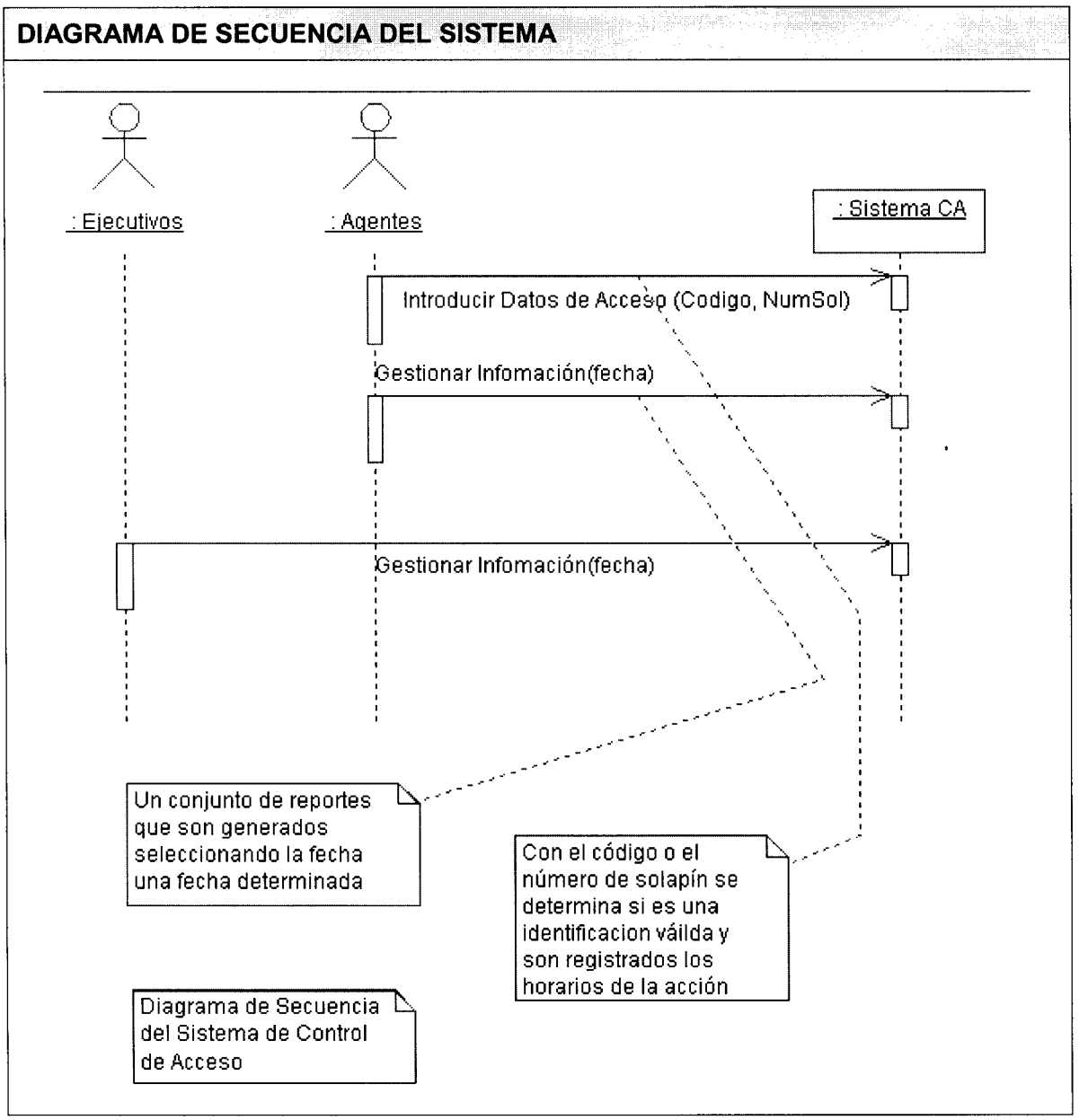
DIAGRAMA DE CLASES DE ANALISIS: GESTIONAR INFORMACION



3.3 Diagrama de Secuencia del Sistema

El diagrama de Secuencia del sistema refleja los tipos de interacción que tienen los usuarios con el sistema como "caja negra" es decir, no importa como funcionan la aplicación "por dentro". La interacción entre las clases y los pasos de mensajes serán vistos más adelante en los diagramas de interacción.

DIAGRAMA DE SECUENCIA DEL SISTEMA



3.3.1 Diagramas de Interacción.

Los diagramas de Interacción son similares a los de secuencia lo que estos sí reflejan la interacción entre los componente y el paso de mensajes entre ellos, estos diagramas ayudan a los desarrolladores en la implementación del sistema, que hacer en cada caso que corresponda.

Diagramas:

1. Diagrama de Interacción Insertar Acceso I y II
2. Diagrama de interacción Gestión de Información
3. Diagrama de clases Web Insertar Acceso
4. Diagrama de clases Web Gestionar información

DIAGRAMA DE INTERACCION: INSERTAR ACCESO

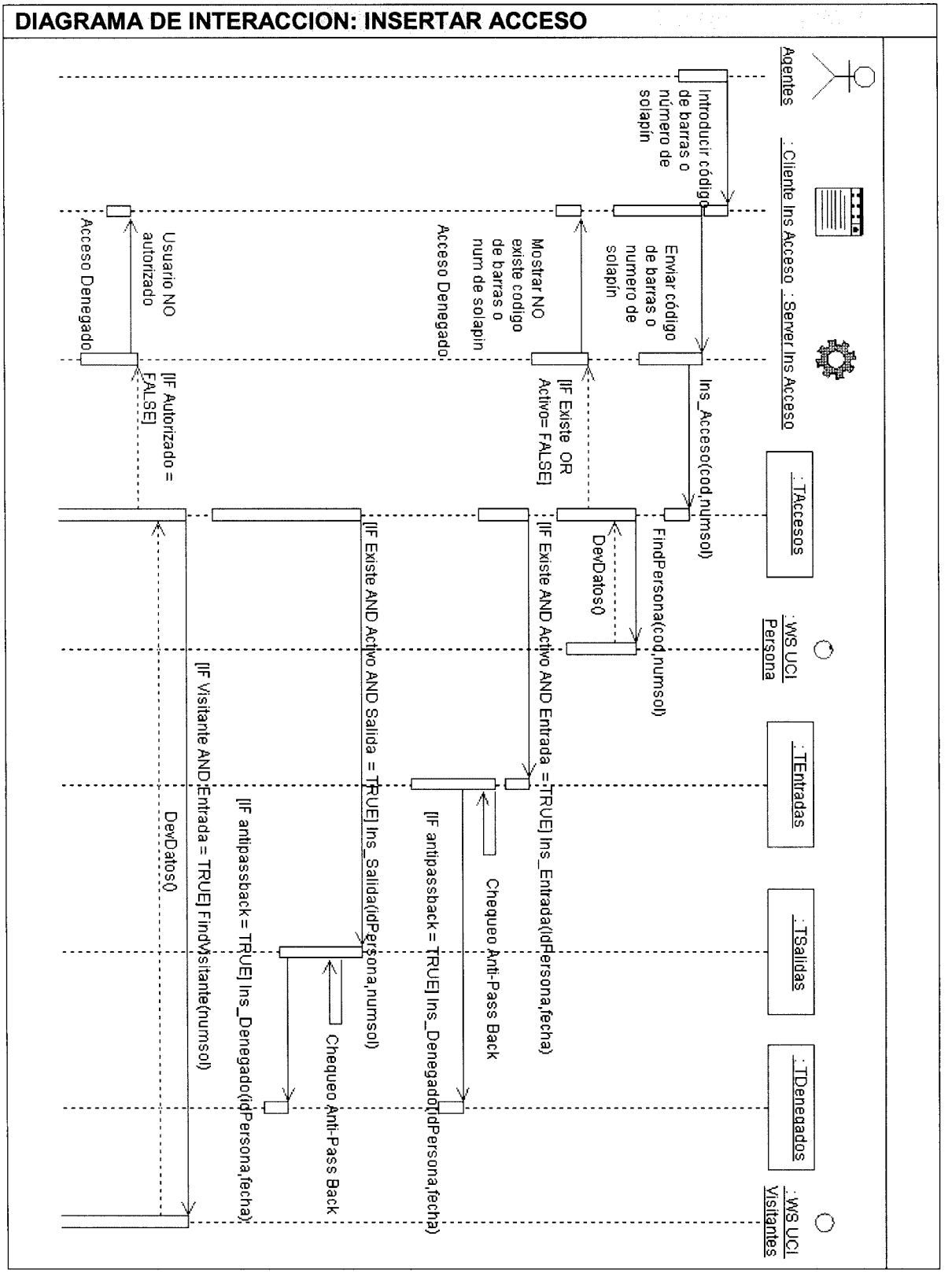


DIAGRAMA DE INTERACCION: INSERTAR ACCESO (II)

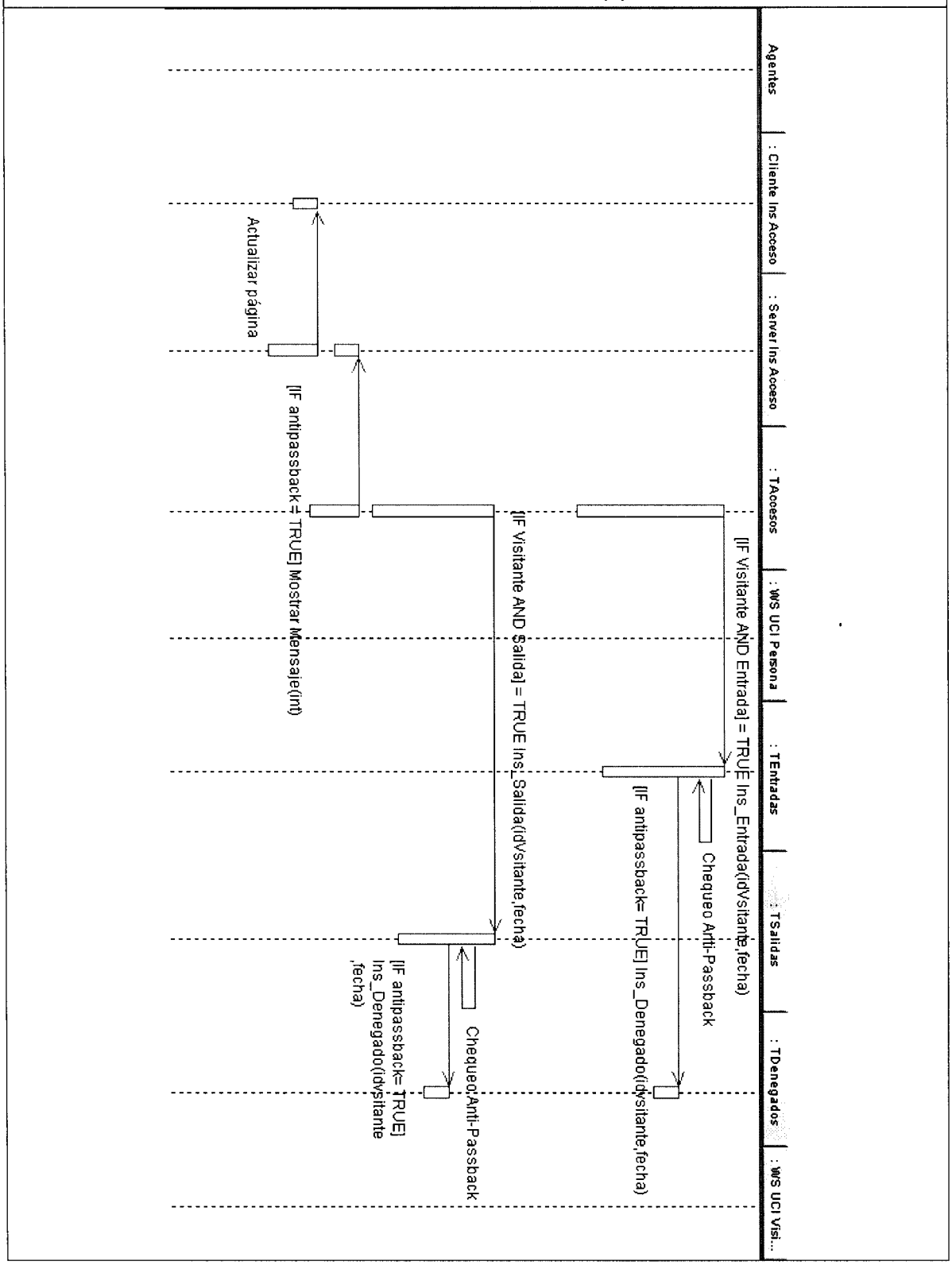
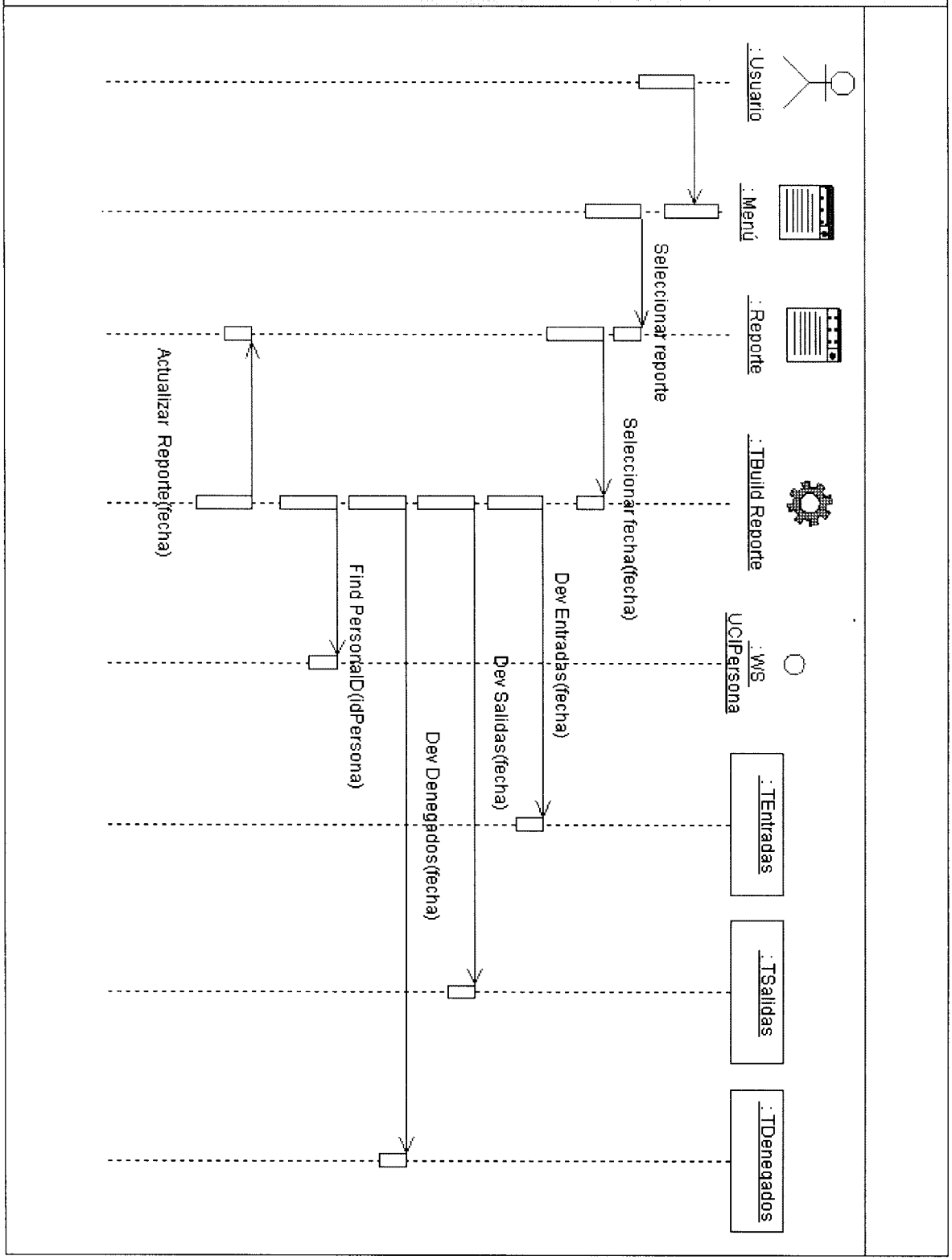


DIAGRAMA DE INTERACCION: GESTIONAR INFORMACION



Nota:

El diagrama de interacción de Gestionar Información anterior sólo hace referencia a un solo servicio Web y es que es sólo para cuando son reportes o consulta de información propiamente de las personas de la UCI, los diagramas de interacción de Gestionar información donde aparecerán los datos de los visitantes, evidentemente tendrán que acceder al servicio Web UCI Visitas, por lo que este diagrama quedaría igual que el anterior solo que la diferencia radica en la clase interfaz WS UCI Persona, serían para las personas UCI y en el caso de los visitantes accedería WS UCI Visita.

DIAGRAMA DE CLASES WEB: CHEQUEO DE IDENTIFICACION

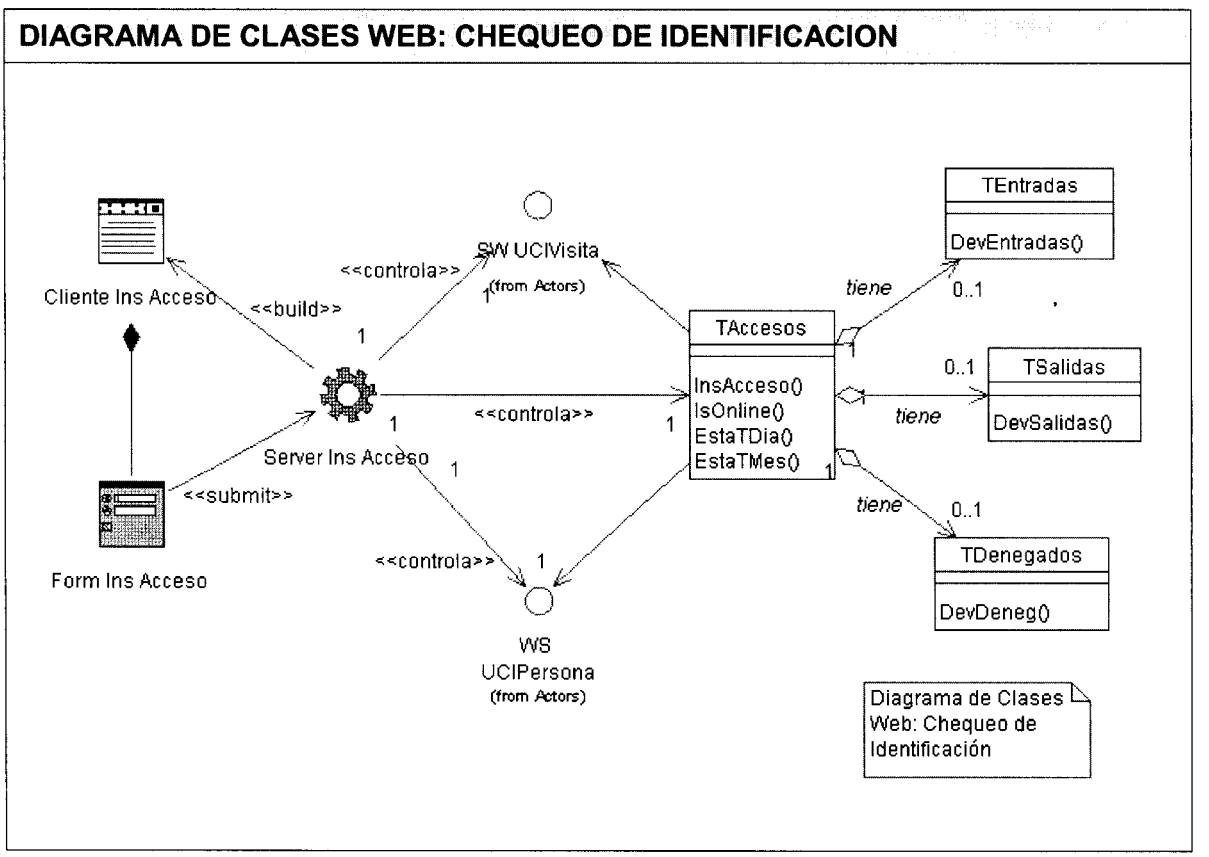
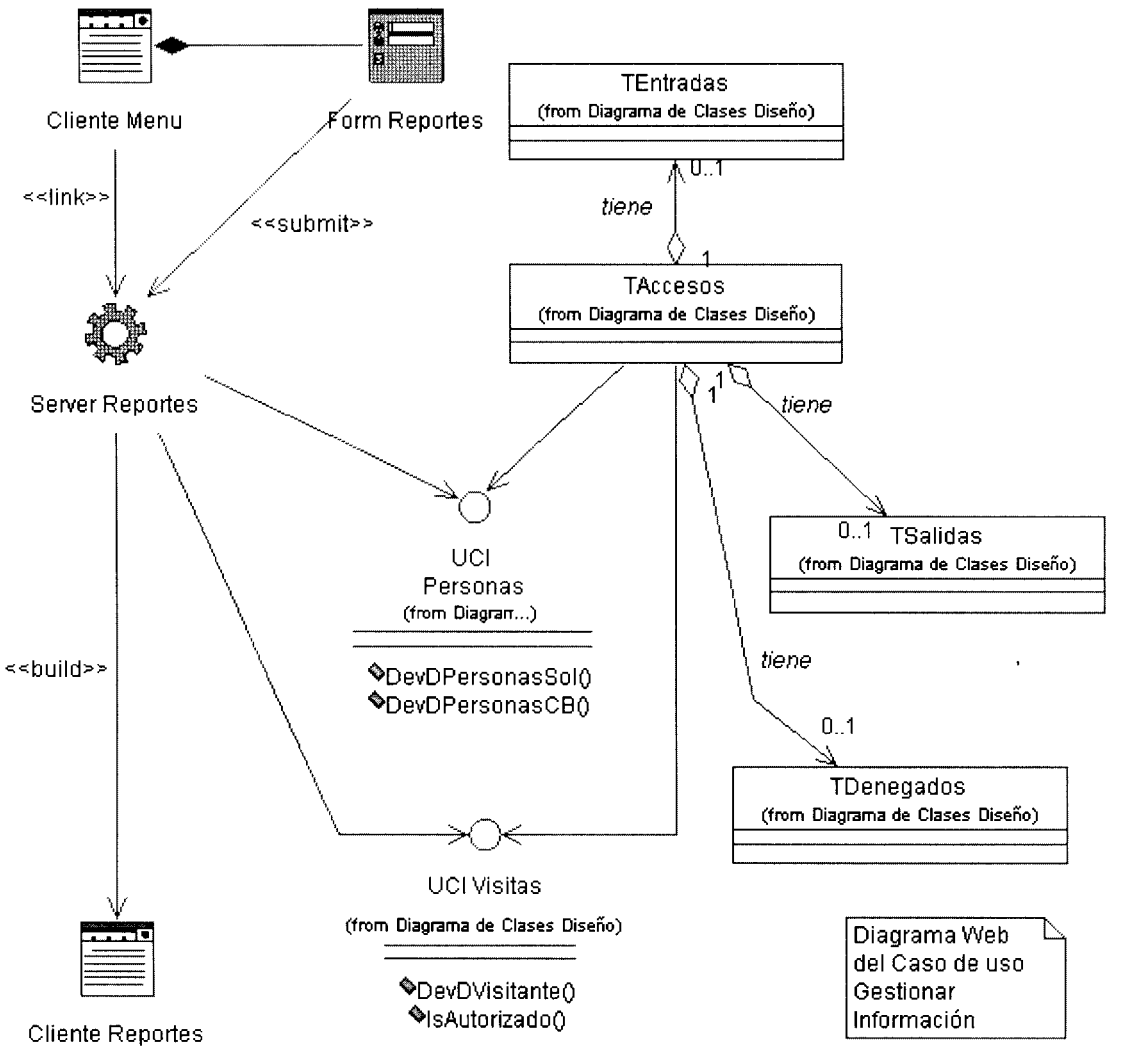
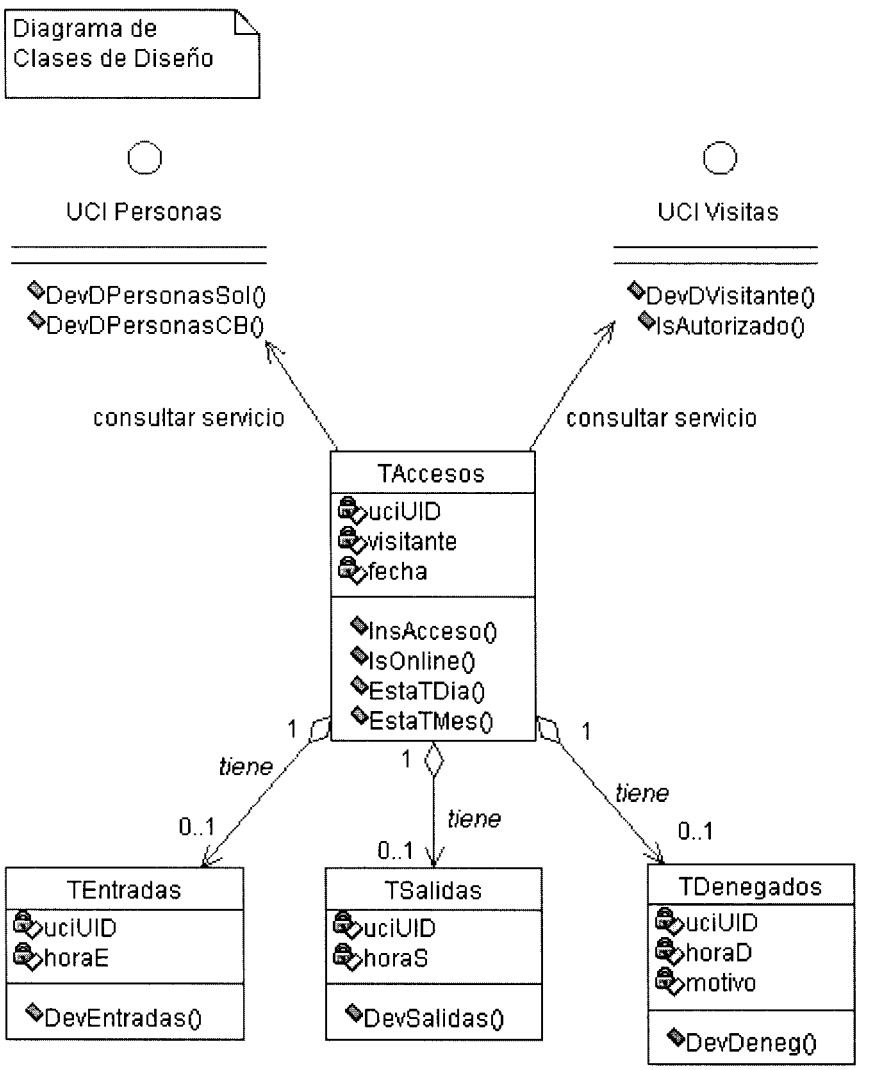


DIAGRAMA DE CLASES WEB: GESTIONAR INFORMACION



3.4 Diagrama de Clases de Diseño

DIAGRAMA DE CLASES DEL MODELO DE DISEÑO



3.5 Descripción de las Clases

CLASE: TACCESOS	
Tipo : Controladora	
Atributo	**Tipo**
uciUID	Nvarchar(36)
visitante	Bolean
Fecha	datetime
InsAcceso(uciUID, entrada(s/n))	
Descripción Responsable de insertar un acceso de entrada o salida, si existe el anti-pass back, entonces inserta un Acceso Denegado.	
IsONLine(uciUID)	
Descripción Responsable de buscar si una persona está "dentro" del sistema (que haya entrado pero que no haya salido), es usado para detectar el anti-pass back.	
EstaTDia(fecha)	
Descripción Responsable de reportar algunos indicadores de los accesos de entrada o salida del día. Cantidades de entrada y salida por tipo, totales, personas Online (dentro sin salida) etc.	
EstaTMes(fecha)	
Igual que el día pero esta vez a nivel del mes.	

CLASE: TENTRADA	
Tipo : Entidad	
Atributo	**Tipo**
uciUID	Nvarchar(36)
HoraE	datetime
DevEntradas (uciUID,fecha)	
Descripción Responsable de acceder a las entradas de una persona en una fecha específica.	

CLASE: TSALIDA	
Tipo : Entidad	
Atributo	**Tipo**
uciUID	Nvarchar(36)
HoraS	datetime
DevSalidas (uciUID,fecha)	
Descripción Responsable de acceder a las salidas de una persona en una fecha específica.	

CLASE: TDENEGADOS	
Tipo : Entidad	
Atributo	**Tipo**
uciUID	Nvarchar(36)
HoraE	Datetime
motivo	nvarchar
DevDeneg (fecha)	
Descripción Responsable de acceder a los datos de las personas que fueron denegados en una fecha específica.	

CLASE: UCI PERSONAS	
Tipo : Interfaz	
Atributo	**Tipo**
…	…
DevDPersonasSol (solapin:int)	
Descripción Esta clase pertenece a la Interfaz de un servicio Web responsable de acceder a los datos de las personas por números de solapín.	
DevDPersonasCB (codigo:nvarchar)	
Descripción Esta clase pertenece a la Interfaz de un servicio Web responsable de acceder a los datos de las personas por código de barras.	

CLASE: UCI VISITAS	
Tipo : Interfaz	
Atributo	**Tipo**
…	…
DevDVisitante (visitante: nvarchar)	
Descripción Esta clase pertenece a la Interfaz de un servicio Web del sistema UCI Visitas responsable de acceder a los datos de las personas que son o han visitado la Universidad.	
Inautorizado (visitante: nvarchar)	
Descripción Esta clase pertenece a la Interfaz de un servicio Web con la que es posible conocer si un visitantes de autorizado o no.	

Nota:

La descripción del campo atributo y tipo están vacías en las dos descripciones anteriores porque realmente no son necesarias, son unos servicios Web los que serán usados, por tanto lo importante aquí son los métodos que están publicados en los servicios Web.

3.6 Diseño de la Base de Datos

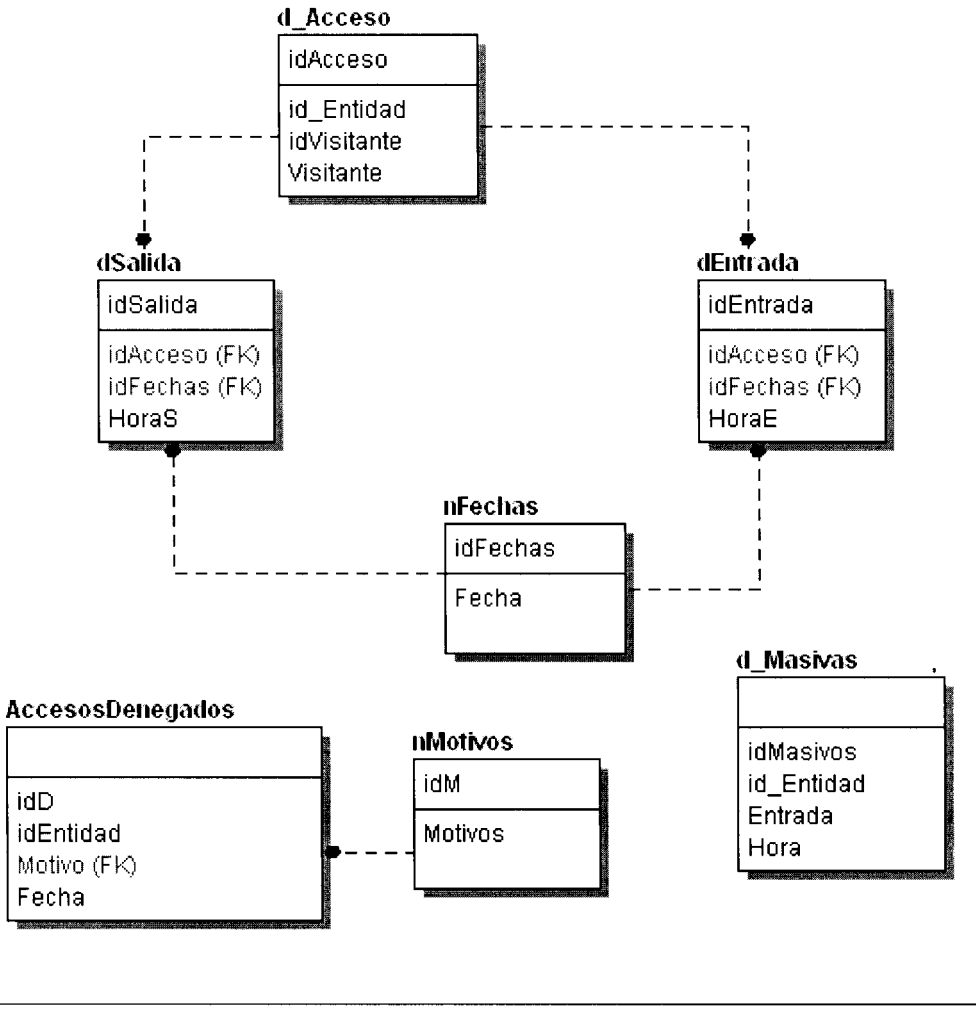
Como ya se ha estado explicando el Sistema de Control de Acceso se valdrá de los datos de la identificación de cada persona que el servicio Web del Sistema de Acreditación le pueda brindar.

Como funciona el anti-pass back a este nivel de base de datos.
Si la persona está entrando se busca que ultima entrada que tuvo ya tenga una salida, sólo así puede volver a entrar, sino luego de reconocer a la persona su identificación sería insertada en denegado y las razones por las que fue insertada.
En la salida igual, sólo que no puede tener salida si esta persona no ha entrada aún.

Una breve explicación de cómo funcionarían las entradas y salidas masivas de personal. Al entrar o salir, así de forma masiva los agentes de seguridad con dispositivos portátiles recolectan todos los códigos de barras de las personas que entran o salen y luego se descargarían estos en un formulario especial para estos fines todos estos datos serán insertados en la tabla "d_Masivas", luego con todos estos datos insertados ahí, un trabajo (Jobs) en el Servidor de Base de Datos, que se ejecutaría cada cierto tiempo ó un en su defecto un disparador(Trigger) que responda al evento de inserción para que, cada vez que sea insertado un registro, repita el proceso de chequeo de identificación y tomaría esos datos para realizar el proceso de chequeo de identificación ya explicado, insertar en entrada si es de entrada y no tiene anti-pass back y salida en salida cuando no tenga anti-pass back, cuando se cumpla un anti-pass back entonces a esa persona la pasamos para la tabla de Accesos Denegados y especificamos el motivo que estos estarán almacenados en la tabla "nMotivos".

Así cuando se quiera saber las posibles violaciones de seguridad o carnet duplicados o cualquier tipo de anormalidad se detectaría chequeando los reportes de los accesos denegados. Y se tomarían medidas con las personas que incurran en estas infracciones.

DIAGRAMA ENTIDAD RELACION



3.6.1 Descripción de las Tablas

NOMBRE: D_ACCESO		
DESCRIPCION: Tabla principal que registra los datos de la persona que está accediendo. Pueden almacenar el identificador de la persona UCI o el identificador del Visitante, tiene un campo booleano que indica si es visitante o no.		
ATRIBUTO	**TIPO**	**DESCRIPCION**
idAcceso	integer	Identificador de tabla
Id_Entidad	nvarchar(36)	Identificador de las personas UCI, únicos en el Sistema de Acreditación.
idVisitante	integer	Identificador de tabla de Visitantes (luego de haber sido aprobado y autorizada su entrada si era un visitante previsto o no)
visitante	bit	Indica si una persona es visitante o no

NOMBRE: NFECHAS		
DESCRIPCION: Tabla que almacena la fecha (una única fecha) en las que ocurren las entradas y salidas.		
ATRIBUTO	**TIPO**	**DESCRIPCION**
idFechas	integer	Identificador de tabla
Fechas	Datetime	Fecha. Con hora, minuto y segundo 0.

NOMBRE: D_ENTRADA		
DESCRIPCION: Tabla que registra el identificador del acceso, de la fecha y el horario de las entradas de la personas a la entrada de la UCI.		
ATRIBUTO	**TIPO**	**DESCRIPCION**
idEntrada	integer	Identificador de tabla
IdAcceso	int	Identificador de la tabla d_Acceso para determinar a cual acceso se refiere esta entrada.
idfecha	int	Identificador de la tabla nFechas (donde se almacenan todas las fechas)
HoraE	Datetime	Campo por defecto (getdate())

NOMBRE: D_SALIDA		
DESCRIPCION: Tabla que registra el identificador del acceso, de la fecha y el horario de las Salida de la personas a la entrada de la UCI.		
ATRIBUTO	**TIPO**	**DESCRIPCION**
idSalida	integer	Identificador de tabla
IdAcceso	int	Identificador de la tabla d_Acceso para determinar a cual acceso se refiere esta entrada.
idfecha	int	Identificador de la tabla nFechas (donde se almacenan todas las fechas)
HoraS	Datetime	Campo por defecto (getdate())

NOMBRE: ACCESOSDENEGADOS		
DESCRIPCION: Tabla que registra el identificador de las personas que incurren en violaciones y el identificador del motivo de esta violación esto sucederá automáticamente cuando sea detectada una violación. Así quedará registrado este evento.		
ATRIBUTO	**TIPO**	**DESCRIPCION**
idD	integer	Identificador de tabla
IdEntidad	int	Identificador de las personas UCI, únicos en el Sistema de Acreditación.
Motivo	int	Identificador de la tabla nMotivos (donde se almacenan la descripción del Motivo)
Hora	Datetime	Campo por defecto (getdate())

NOMBRE: NMOTIVOS		
DESCRIPCION: Tabla que almacena la descripción de los motivos de las violaciones.		
ATRIBUTO	**TIPO**	**DESCRIPCION**
idM	integer	Identificador de tabla
Motivos	nvarchar(50)	Descripción de la violación.

NOMBRE: D_MASIVAS		
DESCRIPCION: Tabla que almacena las entradas o salidas masivas, temporalmente.		
ATRIBUTO	**TIPO**	**DESCRIPCION**
idMasivos	integer	Identificador de tabla
Id_Entidad	nvarchar(36)	Identificador de las personas UCI, únicos en el Sistema de Acreditación
Entrada	boolean	Especifica si es entrada o salida
Hora	Datetime	Hora en la que se realizó la acción

Conclusiones

De manera general los objetivos del trabajo que cumplieron, que fue el de resolver la situación problémica de la Universidad de las Ciencias Informáticas con respecto al Control de Acceso de su personal y el personal externo al centro.

Que quede esta documentación para futuras modificaciones al sistema de Control de Acceso o para el estudio del mismo.

El sistema de Control de Acceso le tributará los horarios de entrada y salida al sistema de Control de Asistencia, así como el mismo se sirve de otros, así se va logrando la interacción entre los sistemas y el nivel de informatización que se quiere lograr en la Universidad.

Recomendaciones

Recomendamos que este trabajo sea tomado como material de consulta por los técnicos o profesionales, que se vayan a enfrentar a un sistema similar o que lo planteado en este trabajo le pueda ser útil en futuros proyectos, así como también puede consultar el resto de la bibliografía que fue utilizada para la confección del mismo.

Referencias Bibliográficas

1. Jacobson I., Booch G., Rumbaught J. "El proceso Unificado de Software". Addison Wesley 2000
2. AURORA bar code technologies (4/4/2004) http://www.dimension-x.com/
3. AURORA bar code technologies. Curiosidades del Código de Barras http://www.dimension-x.com/codefact2.htm
4. Análisis y comparativa de las alternativas propuestas para la Gestión Basada en Web http://jungla.dit.upm.es/~jlopez/publicaciones/jitel01.pdf (10/6/2004)

Bibliografía Consultada

1. Fowler, Martín. "UML Gota a Gota". Primera Edición. Addison Wesley Longman. 1999.

2. Larman, Craig. *UML y Patrones, Introducción al análisis y diseño orientado a objetos*. Prentice-Hall, 2002.

3. Ceria, Santiago. *Ingeniería de Software I. Casos de Uso. Un Método Práctico* para Explorar Requerimientos.

4. Desarrollo basado en RUP bajo la herramienta Rational Rose http://lml.ls.fi.upm.es/mdp/si/ (4/4/2004)

5. Universidad .NET http://www.microsoft.com/spanish/msdn/comunidad/uni.net/ (4/4/2004)

6. Curso práctico de desarrollo de aplicaciones con Visual Studio .NET http://www.microsoft.com/spanish/msdn/comunidad/uni.net/ (4/4/2004)

7. Villariño, Luis. *UML para Web*. 2002.

8. Booch, G., Rumbaugh, J., Jacobson, I. *El Lenguaje Unificado de Modelado*. Addison-Wesley. 1999.

9. Booch, G., Rumbaugh, J., Jacobson, I. *The Unified Software Development Process*. Addison-Wesley. 1999.

10. Cockburn, A. *Using Goal-Based Use Cases*. JOOP, 1997

11. García Molina, J. *Towards Use Case and Conceptual Models through Business Modeling*. Conference on Conceptual Modelling. 2000

12. Larman, C. *Applying UML and Patterns. An Introduction to Object-Oriented Analysis and Design*. Prentice-Hall, 1998.

13. Gamma, E. *Design Patterns, Elements of Reusable Object-Oriented Software*. Addison-Wesley. 1995.

14. Meyer, B. *Construcción de software orientado a objetos*. Prentice-Hall. 1998.

15. Jim Conallen. *Building Web Applications with UML*. Addison-Wesley. 1999.

Anexos

1. Curiosidades del Código de Barras
2. Comparativa entre las tecnologías de más utilizadas en el control de acceso

ANEXO 1: CURIOSIDADES DEL CODIGO DE BARRAS

"...un capturista comete en promedio un error por cada 300 caracteres tecleados? En comparación, las posibilidades de una lectura errónea de un código de barras están entre una en un millón y una en un trillón.

...el código de barras más conocido es el UPC (Universal Product Code), que actualmente se encuentra en la mayoría de los productos de ventas al consumidor en Norteamérica? Contrario a la creencia popular, el código UPC no contiene el precio del producto, sino una clave única que lo identifica.

...una "light pen" (apuntador tipo pluma) y una "bar code wand" (lector tipo pluma) son cosas completamente diferentes? El término "light pen" se usa para definir al dispositivo que permite al operador dibujar o seleccionar objetos directamente en la pantalla de una computadora. No se trata de un lector de código de barras.

...la primera lectura de un código de barras en una aplicación comercial se llevó a cabo en 1974 en Troy, Ohio, E.U.A., en el supermercado "Marsh´s", al pasar un paquete de chicles Wrigley´s por un lector?

...el término "barcode", en inglés, está mal escrito? La manera correcta es utilizar dos palabras, "bar code".

...los códigos de barras se leen en una sola dimensión? Esto es, únicamente el ancho de las barras y de los espacios es relevante. La altura proporciona al símbolo redundancia y facilita la lectura.

...existen alrededor de cien simbologías ("idiomas") diferentes de código de barras? Sin embargo, sólo media docena son utilizadas regularmente. Estas son Código 39, Codabar, UPC/EAN, Intercalado 2 de 5 y Código 128.

...los lectores láser operan a una velocidad de 40 rastreos por segundo?" [3]

ANEXO 2: TABLA COMPARATIVA DE TECNOLOGIAS MAS USADAS EN EL CONTROL DE ACCESO

COMPARACIONES TECNOLOGICAS			
Tecnologías	Código de barras, banda magnética o proximidad	Biometría "Handpunch"	Conclusiones
Identificación	Sistema de tecnología de punta, que incluye comunicación por puerto ethernet, tiene capacidad de crecimiento en memoria.	Sistema de tecnología de punta, con opción de comunicación por puerto ethernet. Tiene capacidad de crecimiento en memoria.	Ambos sistemas cuentan con opción electrónica actualizada, sólo que el biométrico es un equipo distinto de reconocimiento, ya que identifica personas, lo cual lo hace más confiable que código de barras, banda magnética o proximidad.
Fraudes	Estos sistemas recono cen OBJETOS, mediante el uso de credenciales con código de barras, banda magnética o tarjetas de proximidad.	Este sistema reconoce PERSONAS, mediante el uso de la forma tridimensional de la mano. (Geometría de la mano)	No es lo mismo reconocer OBJETOS, que reconocer PERSONAS.
Velocidad	Con estos sistemas, cualquier persona puede prestar su credencial para que otra persona cheque su asistencia, horas extras, etc.	Estos sistemas pueden ofrecer un tiempo de respuesta en el registro de puntualidad y asistencia entre tres y seis segundos, dependiendo del equipo que se utilice.	En ocasiones es importante el tiempo de respuesta y la velocidad que los equipos ofrecen, pero se tiene que considerar la veracidad del registro final, el cual se puede obtener en dos segundos (identificación de objetos, no se sabe quién lo hace) o en seis segundos (identificación de personas, único por empleado).
Mantenimiento	Las fallas más comunes en estos equipos ocurren en el teclado, en caso de que venga incluido, y en la base de deslizamiento de la credencial, la cual se desgasta con el tiempo. Solo requiere de limpieza general y en especial el área de lectura del código de barras o de la cabeza lectora en banda magnética. Proximidad requiere muy poco mantenimiento.	Las fallas más comunes en estos equipos ocurren en el teclado, el cual tiene movimiento mecánico y también, la base de posición de la mano, la cual puede desgastarse con el uso. Sólo requiere de limpieza general y en especial en la base donde se coloca la mano y los espejos	En ambos casos, las fallas más comunes se pueden corregir con un mantenimiento preventivo o en caso de ser correctivo, estas piezas son consumibles normales. También, en ambos casos, este material es una refacción poco costosa y fácil de remplazar.
Vandalismo	Los sistemas de código de barras o de banda magnética pueden ser dañados, metiendo objetos en la ranura del lector, rociándoles algún líquido o simplemente	Estos sistemas pueden ser dañados, si se les rocía algún líquido o si se rompen sus espejos y/o postes, también si son agredidos físicamente	Entre más restrictivo sea un equipo, más susceptible será al vandalismo, ya que representará mayor obstáculo a las personas que lo utilizan.

	agrediéndolos físicamente, mientras que en los lectores de proximidad, el vandalismo es muy reducido.		
Costos	Según la calidad del equipo y de las funciones que incluyan, se pueden conseguir desde los $1,000.00 US hasta los $8,000.00 US	Un equipo Biométrico para 512 usuarios, tiene un costo desde $1,800.00 US. Dependiendo de la aplicación en que se vaya a instalar.	Los costos son siempre importantes en la toma de decisones para la adquisición de un equipo. Siempre se deberá tomar en cuenta aspectos como: ¿Qué se desea controlar? ¿Cuál es la seguridad que se desea tener en la veracidad de la información?, etc. De tal forma que en una tabla de comparativo costo-beneficio, se obtenga la mejor decisión para una compañía.
Costos Consumible	En un sistema de código de barras, banda magnética o proximidad, se pueden elaborar credenciales con precios desde $1.00 U.S., hasta los $15.00 U.S., dependiendo de la tecnología a utilizar.	En un sistema biométrico el costo del consumible es de $0.00, ya que la mano no le cuesta a la empresa.	En cada proyecto de puntualidad y asistencia, si éste es de código de barras o cualquier otra tecnología que identifique objetos, se debe considerar un 30% adicional a las credenciales que se necesiten, ya que la rotación y las pérdidas necesitarán de reposición inmediata. En un biométrico no se da este caso.

Glosario de Términos

anti-pass back

se produce cuando es detectado dos acciones iguales, es decir, en nuestro caso, 2 entradas para que pueda ocurrir la otra entrada, tiene que haber primero una salida.

bacth

lote, por lotes.

Palm Pilot, Palm Top

cumple la función de un asistente personal con una capacidad de trabajo similar a la de una computadora. No tienen teclado, para ingresar datos y desplazarse entre íconos y programas, debe accionarse un stylus o lápiz plástico contra la pantalla, sensible al tacto.