UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

TARJETAS INTELIGENTES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERA EN COMPUTACIÓN

P R E S E N T A N :

CANCINO RAMÍREZ GABRIELA SUSANA

CORTÉS CABRERA CLAUDIA

DIRECTOR DE TESIS:

DR. SAÚL DANIEL SANTILLÁN GUTIERREZ

MÉXICO, D. F. **2005**

Dedicatorias

A mi madre que me dio la fortaleza para mantenerme firme aún en los momentos más difíciles. ¡Gracias Mamá por no dejarme renunciar a este sueño!

A mi padre que siempre me ha inculcado que la mayor herencia que se le puede dar a un hijo es una profesión, he aquí una pequeña parte de esta herencia, ¡gracias papá!

A mis hermanos Nallely, Enrique y Mauricio, mis compañeros de toda la vida, a quienes he enseñado, de quienes he aprendido y con quienes he compartido tantos momentos especiales, ¡los quiero mucho!

A mi asesor de Tesis quien confió plenamente en todos los que participamos en este proyecto, gracias Dr. Saúl por compartir con nosotros sus experiencias, conocimientos y amistad!

A Gerardo, Javier, Serafín y Luis que formaron parte de este proyecto, porque cada uno de ustedes me permitió crecer profesionalmente. Con ustedes aprendí a trabajar en equipo, y aún cuando la convivencia llegó a tornarse complicada aprendimos a superarla satisfactoriamente y con muchas experiencias importantes.

A mi compañera de Tesis, con quien compartí esta experiencia tan enriquecedora. Claus, tú mejor que nadie sabe el tiempo y la dedicación que necesitamos para llegar hasta aquí. Me dio muchos gusto poder trabajar contigo y conocerte tan profundamente, ¡gracias amiga!

A Gonzalo, quien formó una parte importante de este proyecto, gracias por apoyarme incondicionalmente y por quedarte a mi lado para formar parte del proyecto más importante de mi vida, ¡te amo!

Gabriela Cancino Ramírez

Dedicatorias

Este trabajo lo dedico especialmente a mi abuela porque aunque ya no esta conmigo nunca he dejado de sentir su amor y apoyo. ¡Abue, mi viejecita chula!, fuiste y seguirás siendo la mujer que más admiro.

A mi mamá. por todo su esfuerzo, empeño y desvelos en lograr brindarme una profesión. ¡Gracias mami, te quiero mucho!

A mi hermana, tía y papá por toda la confianza, paciencia y apoyo que me brindan. ¡Gracias, los quiero mucho¡

A todos los que participaron en el proyecto: Dr. Saúl Santillán, Serafín, Luis, Javier y Gerardo porque gracias a su valioso trabajo es que todo fue posible.

A mis amigos de la Facultad porque sin ellos la carrera no hubiera sido lo mismo...¡Fabysr, Marco, Isra, Liz, Jaque, Mago, Ara y Gaby, gracias por su amistad!

A mi compañera de tesis: Gaby, eres el mejor equipo que pude tener. Hemos pasado por muchas cosas que estoy segura nos han hecho crecer a nivel personal y profesional. ¡Gracias por ser tan amiga, te estimo muchísimo!

Y por supuesto que a ti Kike, porque siempre estas a mi lado. ¡Te amo!

Claudia Cortés Cabrera

Contenido

Prólogo

El presente trabajo de tesis expone el diseño, desarrollo y puesta en operación de un software llamado: Sistema de Acceso para Personal y Equipo también conocido como SAPPE por sus iniciales.

Dicho software forma parte de un proyecto mayor, cuya finalidad es garantizar la seguridad de algunas de las instalaciones de la Facultad de Ingeniería. El proyecto básicamente se trata de un sistema de seguridad integrado por diversos dispositivos basados en tecnología de radiofrecuencia.

Así el objetivo primordial es desarrollar una aplicación capaz de controlar todos esos dispositivos y proveer una interfaz entre el usuario y el sistema de seguridad.

Para lograr ese objetivo primario junto con algunos otros objetivos surgidos de las necesidades de los usuarios. Se efectuaron varias actividades, cada una de las cuales se detalla a lo largo de los capítulos que integran este documento.

En el primer capítulo de esta tesis se abordan los conceptos básicos que requiere el desarrollo de un sistema de seguridad y las diferentes tecnologías existentes. Con esto se pretende proporcionar el marco teórico necesario para tener una concepción general del proyecto.

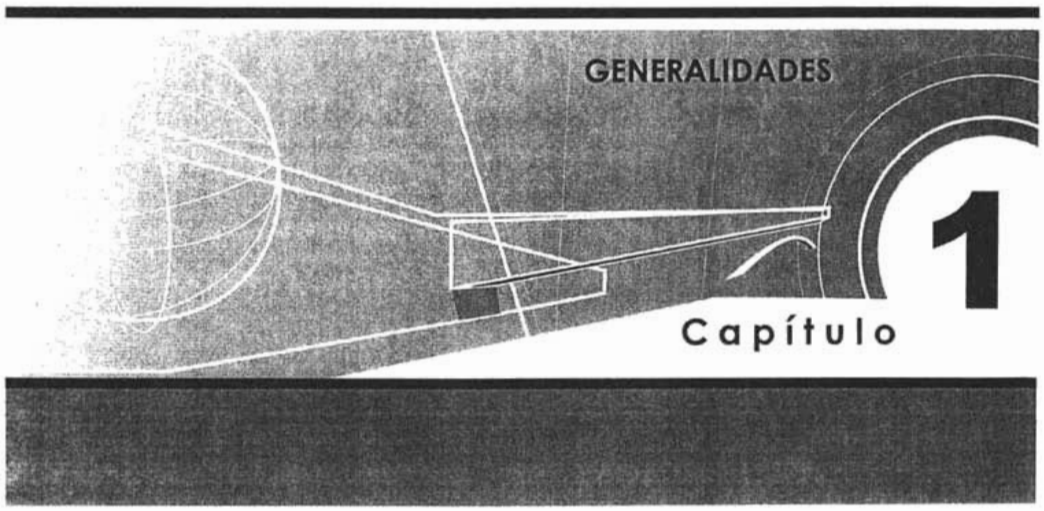
Una vez expuestos los conceptos básicos, el capítulo 2 delimita el alcance de la tesis con una descripción detallada del proyecto. Se presentan las circunstancias bajo las cuales surge la necesidad creación de un software de propósito específico. Así como las características y requerimientos de usuario que deberá cumplir dicho software. Al final del capítulo, en forma de tabla se aprecia la solución propuesta.

El capítulo 3 se refiere al diseño de la aplicación. Se presentan los módulos de los que estará compuesto el software, las relaciones entre módulos y a detalle el funcionamiento esperado de cada uno de ellos. También, se describen la lógica de operación de los dispositivos de hardware que se controlaran así como el plan para implementar dicha lógica en el software. Y por último se define la Base de Datos de la aplicación mediante diagramas entidad-relación.

Una vez definida la aplicación en su totalidad, el capítulo 4 se enfoca a los detalles de programación.

El capítulo 5, detalla las etapas que se llevaron a cabo para la puesta en operación del proyecto. Desde la instalación de los componentes de hardware y software, pasando por los diversos tipos de pruebas efectuados, hasta la elaboración de manuales y cursos de operación que fueron dados a los usuarios. También se incluye el plan de mantenimiento y algunas sugerencias de posibles mejoras a la aplicación para futuros desarrollos.

Para finalizar este documento se presentan las conclusiones del proyecto, incluyendo en ellas los objetivos alcanzados, problemas durante el desarrollo y los logros obtenidos.


GENERALIDADES
1
Capítulo

Capítulo

1

GENERALIDADES

1.1 Introducción

A través de los tiempos, el hombre siempre ha encontrado la forma de garantizar su supervivencia satisfaciendo desde sus necesidades básicas como la alimentación hasta evitando riesgos innecesarios que pongan en peligro su vida. Así el concepto de seguridad ha estado siempre presente aunque de manera implícita en la vida humana:

"Seguridad: f. (lat. Securitis). Confianza, tranquilidad de una persona procedente de la idea que no hay ningún peligro que temer. Protección contra determinados riesgos"[1]

Ingeniosos métodos para señalar y evitar peligros se han ocupado durante siglos. Las señales de humo que empleaban los indios para dar aviso de algún extraño divisado a lo lejos, el empleo del repiqueteo de campanas para indicar siniestros como temblores, invasiones o inundaciones en las pequeñas poblaciones y el uso de trancas de madera para asegurar las puertas son sólo algunos ejemplos. Pero , cientos y cientos de ideas han surgido a lo largo de la historia con el único objetivo de garantizar la protección tanto de la vida como de los bienes materiales.

Es hasta nuestros días en que con el tipo de vida de las sociedades modernas en que diversos peligros como atracos o incendios son parte de la cotidianidad , que los primeros sencillos artilugios que garantizaban protección ya no son suficientes y se han ido complicando y combinando de tal forma que surgen los llamados sistemas de seguridad e incluso se considera al tema de la seguridad, ya no como un tópico más sino como todo una disciplina con un amplio campo de estudio.

Un Sistema de Seguridad, de manera general, se puede definir como el conjunto de dispositivos, instalaciones y lineamientos necesarios para proporcionar protección tanto a personas como a bienes materiales contra determinados riesgos, en un local particular.

[1] "Seguridad". Pequeño Larousse en Color. Ramón García-Pelayo y Gross. Ed. Larousse. España, 1990

1.2 Sistemas de Seguridad

1.2.1 Evolución de los Sistemas de Seguridad

La evolución de los Sistemas de Seguridad desde sus orígenes a la fecha se ha encontrado estrechamente ligado a la invención de nuevas tecnologías, de hecho es en recientes décadas, que con el surgimiento y acelerado avance de la electrónica e informática se ha dado un marcado adelanto en esta industria.

El principio de los Sistemas de Seguridad se puede remontar hasta las rudimentarias técnicas de protección de casas tales como el uso de cerraduras y barrotes en las ventanas. La cerradura más vieja de la que se tiene noticia fue encontrada por arqueólogos en las Ruinas del Palacio de Khorsabad cerca de Nineveth y se estima en 4000 años de edad.

Conforme las civilizaciones fueron avanzando incluso surgieron entidades específicas , autoridades responsables por la seguridad como la policía y las agencias de protección contra incendios, sin embargo, fue hasta finales de la Era Industrial que se tiene noticia de los primeros Sistema de Seguridad. Estos sistemas no contaban con una forma de almacenar los registros de acontecimientos y únicamente eran impresos en las centrales de las compañías. Es en esta época también surgen las primeras agencias privadas expertas en servicios de seguridad , destacan las fundadas por Philip Sorensen en Suecia y Allan Pinkerton en Estados Unidos.

Algún tiempo paso sin avances significativos y es hasta los años de la Primera y Segunda guerra Mundial que se desarrollo mucha tecnología necesaria para la guerra, la cual posteriormente fue aprovechada en todos los demás ámbitos.

La Era de la Información trajo consigo importantísimos avances desde surgimiento de la computadora, ciruitos integrados hasta sofisticados dispositivos sensores, que agregaron a los sistemas de seguridad posibilidades antes inimaginables como la detección automática de riesgos, comunicación remota y almacenamiento masivo de los registros de eventos ocurridos.

Hoy en día, la tendencia en la industria de la seguridad, es crear sistemas con un alto grado de integración e interoperabilidad aprovechando la inercia de la electrónica en construir dispositivos cada vez más pequeños y el surgimiento de nuevas tecnologías.

1.2.2 Objetivos de los Sistemas de Seguridad

Todo Sistema de Seguridad tiene como principal objetivo cumplir con la idea básica del concepto de seguridad, "la protección" con este fin, realiza una serie de acciones fundamentales:

- Detectar
- Impedir
- Señalar
- Evaluar y Actuar
- Neutralizar

Detectar

Cualquier evento que se haya sido clasificado como de riesgo al momento de diseñar el sistema debe poder ser detectado, esto puede ir desde la entrada de instrusos a un local determinado hasta un incendio

Impedir

En principio, ante un evento de riesgo, lo que buscará el sistema es impedirlo, por ejemplo para evitar la entrada de intrusos a un local determinado puede contemplar la instalación de rejas y cerraduras.

Señalar

No basta con detectar que algo pasa, es necesario informar de la situación a los responsables, esto se logra mediante el empleo de alguna señal ya sea visual o audible, por ejemplo una alarma.

Evaluar y Actuar

El sistema además debe poder valorar la situación y en base a ello tomar las medidas pertinentes encaminadas ya sea ignorar, disminuir o neutralizar los efectos de lo ocurrido.

Neutralizar

Existe un poco de polémica respecto a este punto, ya que no todos los autores consideran la acción de neutralizar como parte del mismo sistema ya que se refiere por lo general a tomar acciones conjuntas con otras entidades como la policía que estrictamente no forma parte del sistema.

Según sean los alcances de un sistema, este cumplirá con uno, algunos o todos los puntos antes mencionados definiendo en base a ello el nivel de seguridad con el que se cuenta.

Nivel de Mínima Seguridad - Impedir
Nivel de Baja Seguridad - Impedir, detectar, señalar
Nivel de Seguridad Medio - Impedir, Detectar, Señalar , Evaluar y Actuar
Nivel de Seguridad Alto – Impedir, Detectar, Señalar, Evaluar y Actuar, Neutralizar

1.2.3 Clasificación de los Sistemas de Seguridad

Hoy en día debido a la gran variedad de posibilidades que la industria electrónica ha añadido al ámbito de la seguridad, el número de aplicaciones en los que se ocupan Sistemas de Seguridad es impresionante, de tal forma que una clasificación minuciosa de los sistemas existentes resulta prácticamente imposible. Sin embargo el uso extendido y prolongado de algunos sistemas populares permite por lo menos una clasificación general, que es la que presentamos a continuación:

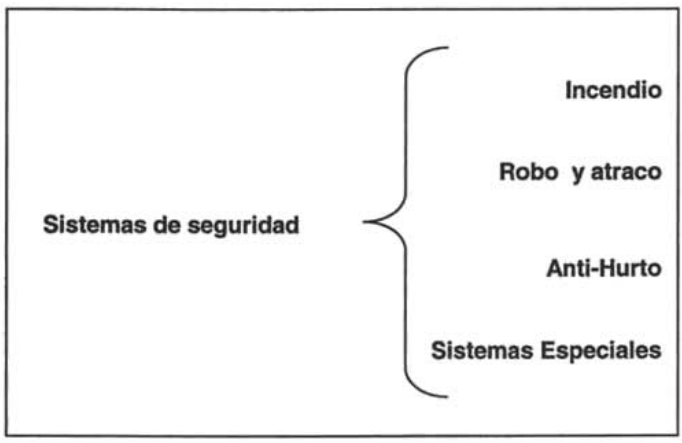


Figura 1.1 Clasificación de los Sistemas de Seguridad

1.2.4 Diseño de Sistemas de Seguridad

Los Sistemas de Seguridad son tan diversos como lo son las necesidades que los originan, esto es que, cada sistema es un caso particular con características y cualidades específicas producto de un amplio análisis de los requerimientos del cliente.

De lo anterior es sencillo apreciar que el proceso de diseño de Sistemas de Seguridad no es tarea fácil ya que siempre se encuentra supeditado a las necesidades del cliente, sin embargo los expertos en el tema coinciden en señalar algunos lineamientos básicos, que facilitan la ardúa labor.

Lo primero es tener bien claro que un buen sistema de seguridad debe ser "holistico", es decir, que abarca absolutamente todos los aspectos relacionados con el mismo sin descuidar ningún detalle, por ejemplo:

"De nada sirve poner una reja corrediza de barras de titanio de quince centímetros de grosor para proteger la entrada de un establecimiento si además no se le pone un candado para cerrarla"[2]

Pero, ¿cómo abarcar todos los aspectos? Esto se logra abordando al problema de seguridad desde un principio por todos los ángulos distintos posibles. El enfoque más ampliamente aceptado es el que considera la solución al problema de seguridad como una serie de pasos que poco a poco llevan a la meta de protección al mismo tiempo que cada paso abarca todas los aspectos involucrados en el sistema, al final logrando redundancia y diversidad.

El primer paso es la definición detallada de lo que se desea proteger, comienza con tres preguntas :

1. ¿Qué es lo que se desea proteger?
2. ¿Qué tan importante es lo que se desea proteger? o ¿Por qué se protege?
3. ¿El costo de la protección excede su valor?

La respuesta a estos sencillos cuestionamientos arroja información valiosa que permite de entrada establecer la meta principal del sistema y considerar si es factible continuar con el diseño, o no. Una vez conocidas las respuestas, es posible pasar a una fase de análisis para este primer paso mucho más detallada.

Posteriormente elaborar una lista detallada de los requisitos básicos del sistema, en base a una previa examinación del local a proteger. Dicha examinación debe identificar el estado actual de la seguridad, señalar las deficiencias actuales y en base a esto determinar la protección requerida. En la lista de requisitos que se efectúe bajo cada uno de ellos, se recomienda colocar todas las posibles opciones

[2] "Definición de una política de seguridad" RedIris , 2003

de tecnología que pudieran contribuir a su cumplimiento, pueden ser desde chapas, sensores, pasando por CCTV (Televisión de Circuito Cerrado) o hasta tecnología de acceso biométrica. Después dependiendo de el nivel de seguridad que se persigue y los recursos disponibles es posible descartar algunos de los dispositivos listados.

El segundo paso también se trata de un análisis sistemático sólo que esta vez para definir todos los posibles eventos de riesgo y sus ejecutantes. La información obtenida hasta este punto se ocupa conjuntamente para elaborar la estrategia de seguridad como se verá más adelante.

En está ocasión aunque este análisis también se apoya en el estudio en sitio. La principal fuente de información debe considerarse, él o los encargados de la seguridad y gente del lugar quienes en base a la experiencia identificarán rápidamente los posibles riesgos y les darán la proporción adecuada. Se elabora una lista de las posibles amenazas a un lugar, posteriormente se organiza en orden de importancia a esta lista le sigue otra pero de los posibles ejecutantes y finalmente se correlacionan ambas listas.

Para este punto los diseñadores ya cuentan con la información necesaria que les permitirá elaborar un buen sistema y los parámetros deseados.

El tercer paso es elaborar un plan de seguridad, quizá es el paso más importante porque hasta el momento únicamente lo que se ha recolectado es información que si bien es valiosa, no sirve de mucho sino se concreta en una clara idea de cómo emplearla para lograr los fines propuestos.

La estrategia de protección abarca, distintos niveles del sistema , que son:

- Nivel Físico
- Humano
- Logístico

Nivel Físico.

Abarca la planeación sobre todas las medidas proactivas, normativas de contingencia y de recuperación en el lugar, que tengan que ver con la parte física del sistema, abarca entre otras cosas:

- Condiciones ambientales internas (por ejemplo localización de zonas vulnerables)
- Condiciones medioambientales (temperatura, húmedad, etc)
- Decisiones de tipos de protección a instalar (por ejemplo controles de acceso)

- Ubicación de dispositivos (sensores , cámaras u otros dispositivos)
- Sistemas de contingencia
  (extintores, fuentes de alimentación ininterrumpida, etc.)
- Sistemas de recuperación (Redundancia, sistemas alternativos, etc.)
- Comunicaciones (Señales de alarma, monitoreos, etc.)
- Interacciones entre los componentes físicos del sistema

Nivel Humano.

Como ningún sistema se encuentra aislado, con este punto se consideran en la elaboración de la estrategia de seguridad todas las posibles relaciones y grados de interacción de los individuos con el sistema, en especial aquellas que puedan ser un foco alerta de "inseguridad para el sistema de seguridad".

En el nivel humano se consideran:

- El administrador o responsable directo del sistema
- Los usuarios del sistema
- Las personas relacionadas pero que no son usuarios
- Las personas ajenas al sistema

Nivel logístico

Este nivel coordinan todos los elementos involucrados con el sistema, tanto a nivel físico como humano, mediante el establecimiento de protocolos de trabajo y políticas de uso. Por ejemplo si un sistema será instalado en un área laborar, el nivel logístico deberá considerar la dinámica laborar y las necesidades de horario de los empleados antes de implantar el sistema.

1.3 Sistemas de Identificación

1.3.1 Tecnologías de identificación

En las últimas décadas, como consecuencia de una constante evolución tecnológica, las actividades del hombre se han hecho cada vez más complejas, acrecentando la necesidad de encontrar formas de automatizar y simplificar muchos procesos de la vida diaria tales como identificación de personas, pagos, manejo de capital, etc. Es así como surgen las tarjetas de identificación por radiofrecuencia como una solución factible a esta problemática. Las tarjetas comienzan a ser utilizadas a partir de la década de los 60's para cubrir esta necesidad.

El uso de estas tarjetas no sólo ha permitido facilitar muchas de las operaciones comerciales y sociales, sino que ha creado las bases para el desarrollo de nuevas aplicaciones y métodos cada vez más sofisticados de garantizar la seguridad física y material de los individuos.

El desarrollo progresivo de nuevas técnicas orientadas al perfeccionamiento y creación de nuevos dispositivos de identificación han dado la pauta para crear sistemas de seguridad más completos.

Para entender esta revolución tecnológica haremos una retrospección en los distintos sistemas de identificación que se han ido gestando como respuesta a las necesidades específicas de una sociedad cambiante.

Cintas Magnéticas.

La cinta magnética esta constituida por una banda plástica cubierta de un delgado material magnético. La técnica de lectura y escritura de este dispositivo se basa en campos electromagnéticos que permiten alinear secuencialmente cambios de polaridad a través de la cinta. Mediante un grabador compuesto de un cabezal magnético la operación de grabado de la cinta se logra alterando la polarización del material magnético que la cubre. Para poder acceder a ésta información, mediante un lector, se van decodificando los cambios de flujo magnético mismos que se traducen en un código binario.

Para convertir la información binaria de las tarjetas magnéticas se hace uso de métodos de decodificación de alto nivel como son: ISO BCD o el ALPHA, que permiten traducir ésta información en caracteres alfanuméricos.

Las cintas magnéticas han sido el precursor de los sistemas modernos de identificación, siendo tal su importancia que hoy en día se siguen utilizando en muchas organizaciones, particularmente de carácter comercial y económico, como son los bancos que utilizan las tarjetas de crédito para realizar transacciones financieras.

La aplicación de las tarjetas magnéticas en las organizaciones bancarias se da a finales de la década de los setenta. Sin embargo, debido a que es un método barato y flexible de almacenar información, el uso de éstos dispositivos en otras operaciones, tales como la identificación y control de personal en las empresas, tarjetas de débito, licencias de conducir, boletos de transporte y aerolíneas, etc. Se ha ido incrementando.

A pesar de que el empleo de éstos sistemas de identificación actualmente es un método efectivo para cubrir muchas de las necesidades de los clientes, presenta una serie de desventajas:

- Debido a que la técnica empleada para el grabado y lectura de información es a través de campos magnéticos, la exposición a campos magnéticos distintos puede alterar o borrar la información contenida en la cinta.
- El material de que están constituidas es susceptible a daños físicos causados por el medio ambiente.
- La capacidad que tiene para almacenar información es baja.
- Puede haber errores en el momento de lectura lo que se traduce en una baja confiabilidad.
- A pesar de que los dispositivos grabadores y lectores son costosos, no impiden que la información contenida en las cintas pueda ser copiada, duplicada o incluso falsificada por otros métodos similares.

Código de Barras

Este sistema de identificación esta formado por un conjunto de líneas y espacios de distinto grosor ordenados paralelamente.

Figura 1.2 Código de Barras

Mediante dispositivos ópticos podemos decodificar esta serie de barras para enviarlas posteriormente a una computadora. Permitiendo de esta manera la identificación y captura automática de objetos de una forma rápida, sencilla y confiable.

Esta tecnología surge como solución a una problemática que enfrentaban las organizaciones comerciales e industriales a principios de la década de los setenta, cuando el manejo de información para realizar el control y manipulación de productos comenzaba a ser concentrado en ordenadores.

Para estandarizar la manera en que se codificaría la información a través del grosor de las barras y espacios, surgieron reglas que dieron origen a un nuevo concepto, simbología. Las simbologías dependen básicamente de la aplicación a la que están orientadas y sus principales características se definen a partir de los datos que manejan: numéricos, alfanuméricos, de longitud variable y fija, discretas, continuas, etc.

Una de las simbologías más usada es sin duda la EAN/UPC, empleada en los centros comerciales para identificar, clasificar y establecer el costo de los productos, su formato es numérico y de longitud fija.

Asimismo se cuenta con otras simbologías de uso común como son:

- Código 39. La primer simbología alfanumérica utilizada con fines industriales.
- Codebar. Cuya aplicación esta orientada a los bancos de sangre y bibliotecas

La diversidad de dispositivos de lectura que se emplean para decodificar la información almacenada mediante la técnica de código de barras, hace de esta tecnología un método flexible y fácil de instalar; entre los periféricos más comúnmente usados se puede mencionar lápiz óptico, scanner, láser de pistola, etc.

La tecnología de código de barras presenta muchos beneficios para la industria en general, permitiendo la identificación de objetos de forma confiable, la impresión de tarjetas de identificación a bajos costos, velocidad de acceso a la información y una fácil implementación del sistema. Estas características han permitido que su uso se extienda hacia muchas actividades del hombre, principalmente las relacionadas con la agrupación y organización de productos, como son bibliotecas, control de inventarios, bancos de sangre, controles de acceso, etc.

Sin embargo, y al igual que las cintas magnéticas, presenta un grave problema, la facilidad con que el código puede ser duplicado, lo que deriva en un impacto negativo para la seguridad.

Biometría

Uno de los principales problemas que enfrentan los distintos dispositivos de identificación es el riesgo de poder ser duplicados. La búsqueda de nuevos métodos que garanticen una autenticación inequívoca e individualizada ha dado lugar al estudio de características y rasgos únicos de cada individuo como son las huellas dactilares, el iris de los ojos, el rostro, la voz, etc. Y es lo que propiamente se define como biometría.

La implementación de dispositivos que permiten identificar y capturar cada unos de estos rasgos particulares son los dispositivos biométricos Estos dispositivos no sólo hacen más fácil el análisis de todas estas características biológicas, sino que permiten establecer las bases para sistemas cada vez más seguros.
Esta tecnología tiene, sin embargo, una serie de desventajas; el costo de los dispositivos es muy alto y la implementación de un sistema biométrico es muy complicado.

Aunque en últimos años debido a una necesidad cada vez mayor por disponer de sistemas eficientes, confiables y, sobretodo, seguros, el estudio de la biometría se ha incrementado como el principal método para la identificación humana.

Dentro de los dispositivos biométricos que se utilizan actualmente encontramos: los lectores de impresión digital (basados en las huellas digitales), escáner de iris, e identificadores de voz.

Aún falta mucho por investigar en ésta área, pero consideramos que en un futuro no muy lejano la combinación de esta tecnología con otros métodos de identificación permitirán preservar la integridad de los individuos y de sus pertenencias de una forma cada vez más segura.

Figura 1.3 Sistema biométrico

1.3.2 Sistemas de identificación por radiofrecuencia (RFID)

La búsqueda de dispositivos que permitieran disminuir los riesgos de fraudes debidos a la falsificación y duplicación de tarjetas; y la facilidad con que éstas podían perder la información o dañarse, ha impulsado nuevas tecnologías para almacenar y recuperar información dentro de nuevos dispositivos.

Un método que ha resultado eficaz y a procurado avances significativos en las tecnologías de identificación es, sin duda, el sistema basado en radiofrecuencias.

La tecnología por radiofrecuencias permite la identificación automática sin contacto, es decir que el proceso de lectura / escritura en el dispositivo ya no se realiza exponiendo directamente el dispositivo de identificación con el periférico de lectura.. Esta innovadora técnica ha tenido gran impacto en el mercado actual, debido a las ventajas que ofrece al cliente, incrementando y diversificando las aplicaciones que se le pueden dar a esta técnica.

Definición de un sistema de RFID

En un material conductor (una antena, por ejemplo) el movimiento de los electrones a través de él genera un campo eléctrico y magnético en forma de ondas que se propagan a través del medio ambiente a la velocidad de la luz. Estas ondas energizadas eléctrica y magnéticamente producen a su alrededor un campo magnético, el cual puede ser captado por un dispositivo receptor (como comúnmente vemos en la antenas de radio, las antenas de televisión y más recientemente los teléfonos móviles).

El campo electromagnético que se produce en el entorno de un dispositivo transmisor y receptor, se caracteriza por la longitud de onda que emite y su frecuencia. La longitud de onda es la distancia, medida en metros, que existe entre los puntos de un ciclo completo de onda; así mismo la frecuencia indica el numero de ondas que pasan por un punto determinado en un segundo, su unidad de medida es los Hertz (Hz). Como se había mencionado la propagación de estas ondas es a la velocidad de la luz (c = 300,000 km/s), matemáticamente se puede hacer una relación de éstos tres elementos, longitud de onda, frecuencia, y velocidad de la luz, descrita en la siguiente fórmula:

$$\textit{longitud de onda}(\lambda) \times \textit{frecuencia} = c$$

Considerando que c es una constante, se puede observar que la relación entre la longitud de onda y la frecuencia es inversamente proporcional, teniendo así transmisiones de baja frecuencia que generan una longitud de onda larga, y transmisiones de alta frecuencia que emiten una longitud de onda corta.

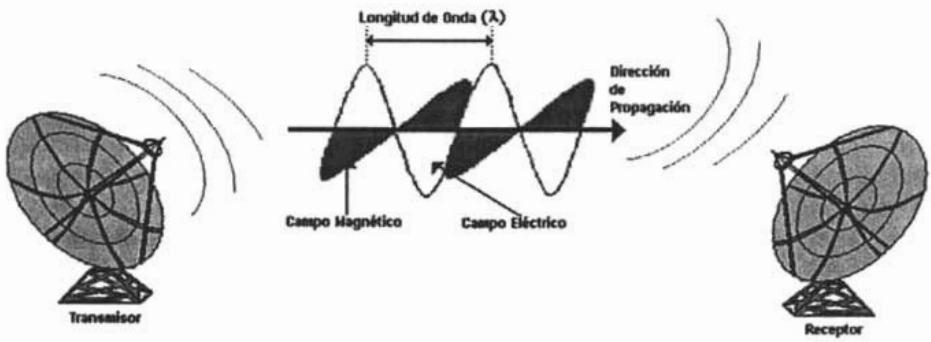


Figura 1.4 Campos magnéticos

Estos principios aportaron grandes beneficios a las comunicaciones sin cable, y más recientemente a la transferencia de datos, lo que dio origen a los sistemas de radiofrecuencia.

Un sistema basado en radiofrecuencia está formado por un conjunto de elementos: antenas, receptores, decodificadores y sistemas de procesamiento de datos, cuyo objetivo es la transmisión de información empleando campos electromagnéticos. Como el manejo de información se hace a través del medio ambiente, ha dado la pauta para revolucionar radicalmente los métodos de captura y transferencia de datos.

Elementos de un sistema de RFID y modo de operación.

El uso de sistemas de radiofrecuencias aplicado a métodos de identificación tradicionales como son las cintas magnéticas y los códigos de barras, generan un sistema de identificación mucho más robusto y seguro, y cuyas aplicaciones se extienden a muchos ámbitos de la vida humana.

La forma en que opera este sistema es principalmente a través de la propagación de ondas electromagnéticas, haciendo uso de tres elementos fundamentales: una unidad de lectura / escritura ("reader"), una antena y un circuito electrónico comúnmente llamado tranponder o tag que permite el almacenamiento de la información. La tecnología utilizada para transmitir y recibir los datos se basa en la radiocomunicación bidireccional de estos elementos.

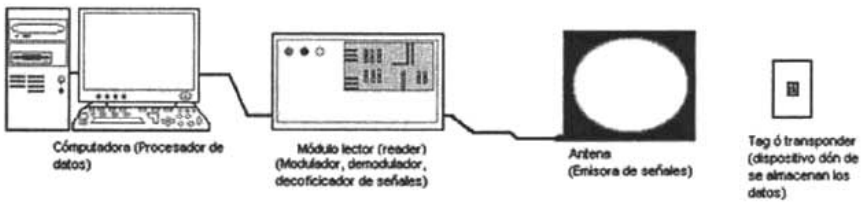


Figura 1.5 Elementos de un sistema de identificación por radiofrecuencia

El principio operativo de este sistema es tan simple como el utilizado en las tarjetas magnéticas y códigos de barras. Sin embargo, la aportación de la microelectrónica ha dado un avance significativo a las tecnologías de identificación.

La unidad de lectura / escritura es el dispositivo central de operaciones del sistema de identificación ya es el que controla la adquisición de datos y comunicación entre la antena y el tag; dispone además de un microprocesador que incrementa sus capacidades y funcionalidad. El microprocesador controla la transmisión de señales de onda a través de la antena, y remodula y decodifica las señales recibidas del transponder, posteriormente envía esta información a una terminal en la cual se procesa la información recibida. Asimismo el microprocesador puede ser reprogramado para realizar tareas adicionales como puede ser el control de otros periféricos como cámaras, alarmas, puertas, etc.

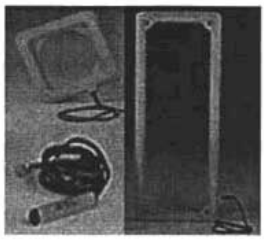


Figura 1.6 Antenas

A través de la antena el "reader" emite señales de radio para activar la lectura y escritura del transpoder. Las antenas pueden ser construidas en diferentes formas y tamaños, adaptándose a cualquier área, por ejemplo el marco de una puerta para monitoreo de personas o bien en un estacionamiento para el control de vehículos.

La antena energizada produce un campo magnético cuya área esta determinada por la potencia generada por el reader, de esta forma si queremos tener un mayor alcance de lectura se debe incrementar la potencia. Posteriormente se debe ubicar el tag en la zona electromagnética para poder realizar la lectura o escritura de datos, éste método permite la captura de datos de forma más sencilla.

La combinación del microprocesador en la unidad lectora y la cobertura que tiene el campo magnético de la antena permite obtener la información de más de un transponder al mismo tiempo a diferencia del código de barras, o las cintas magnéticas en donde sólo podemos leer una etiqueta a la vez.

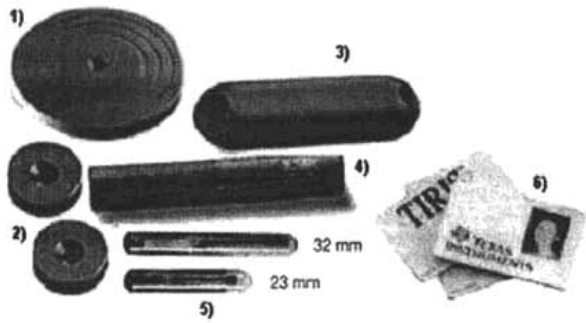
El transponder o tag esta constituido por un dispositivos receptor (antena), un circuito de control (microchip) y una unidad de memoria para almacenar la información. El transponder es un dispositivo receptor y transmisor, de hecho su nombre deriva de la conjunción de las palabras en inglés "**trans**mitter" y "**responder**". A través de la antena integrada recibe las ondas de radio, mismas que son demoduladas en el circuito de control; en respuesta a esta señal el tag transmite la información almacenada en la unidad de memoria en forma de ondas electrónicas que son captadas la antena y enviadas al lector. La forma de acceder a los datos ocurre de forma autónoma, ya que no requiere confrontar directamente el tag con el dispositivo lector, únicamente se debe ubicar en la periferia del campo magnético generado por la antena principal, y la unidad de control actuará de modo automático. Este proceso disminuye considerablemente el tiempo de respuesta.

El uso de un microchip en el transponder ofrece grandes ventajas sobre otros dispositivos, principalmente una capacidad mucho mayor de almacenamiento de información, permitiendo un rango mayor de códigos de identificación que elimina el riesgo de datos duplicados. Así mismo cuentan con un número único de identificación de fábrica, que elimina los riesgos de realizar un fraude a través de la copia o duplicación del dispositivo.

Los transponders se clasifican como activos o pasivos de acuerdo al modo en que adquieren energía para activarse. Los dispositivos activos tienen integrada una batería y se caracterizan por ser de lectura/escritura. A diferencia del código de barras, la información capturada puede ser reescrita y/o modificada, por lo que los dispositivos activos tienen la posibilidad de ser reutilizados. Para garantizar la seguridad y confiabilidad del código de identificación la información puede ser encriptada.. Una de las características de mayor trascendencia de éstos dispositivos es el amplio rango de lectura que ofrece, sin embargo se enfrenta a dos desventajas su alto coso y un máximo periodo de vida de 10 años; aunque considerando el gran crecimiento tecnológico que han tenido, no dudamos en que pronto estas desventajas puedan ser superadas.

Por otra parte en los tags pasivos la energía para activarse es suministrada por el campo magnético generado por la antena. Y a diferencia de los tags activos, éstos son mucho más ligeros y económicos, sin embargo, el rango de lectura es mucho menor.

Actualmente las dimensiones de estos circuitos electrónicos se han reducido a tal grado de ser casi imperceptibles, esto ha permitido que su encapsulamiento adopte una diversidad de formas, tamaños y materiales. De esta manera encontramos transponders en forma de discos, tubos, llaveros, etc. Así mismo la trascendencia que han tenido en los sistemas de identificación han incrementado la producción y desarrollo de nuevos dispositivos orientados a la radiofrecuencia con un costo cada vez menor.



1) Transponder disco fino

2) Transponder tipo disco

3) Transponder para ser montado sobre metal

4) Transponder tipo cilindro

5) Transponders encapsulados en vidrio

6) Transponder tipo tarjeta o etiquetas

Figura 1.7 Tipos de transponders

El perfeccionamiento de los sistemas de radiofrecuencias se incrementa día con día, por lo que podemos encontrar dispositivos con un alcance máximo de activación cada vez mayor y un el incremento en la capacidad de interactuar con un mayor número de señales.

La disminución en costos y el mejoramiento de estos sistemas ha ampliado su campo de aplicación teniendo hoy en día un sin fin de actividades en donde podemos encontrarlos:

- Supervisión de artículos y objetos para evitar el robo de los mismos.

- Monitoreo en producción y transportación. Sin duda ha sido de gran utilidad en las industrias para llevar el control de los productos al ser identificados, permitiendo crear un inventario automatizado. Y protegerlos al ser transportados rastreándolos a lo largo de su trayectoria.

- Control de acceso al personal. El sistema de radiofrecuencia permite de un modo más seguro, confiable y exacto el registro de acceso de personal. Para el personal resulta un método mucho más cómodo, al disminuir el tiempo de espera durante su autenticación y el no tener que presentar su identificación directamente con el dispositivo lector.

- Control de animales. Principalmente podemos ver su uso en la identificación de ganado y para el control de sujetos de laboratorio.

- Acceso y control vehicular. Debido al amplio rango de lectura de estos dispositivos, podemos registrar el acceso de vehículos, por ejemplo, en un estacionamiento o para monitorear del flujo de vehículos en una zona.

- Sus aplicaciones se han extendido también a actividades recreativas, por ejemplo, para establecer nuevas técnicas para cronometrar actividades deportivas registrando distancias y posiciones.

Los sistemas de identificación por radiofrecuencias han demostrado ser hoy en día uno de los métodos más eficaces, seguros, confiables y exactos para poder identificar y proteger la integridad de las personas y de sus bienes, independientemente de todas las aplicaciones que se le puedan dar. Basándonos en estos hechos hemos creado el sistema al que haremos referencia a lo largo de este documento.

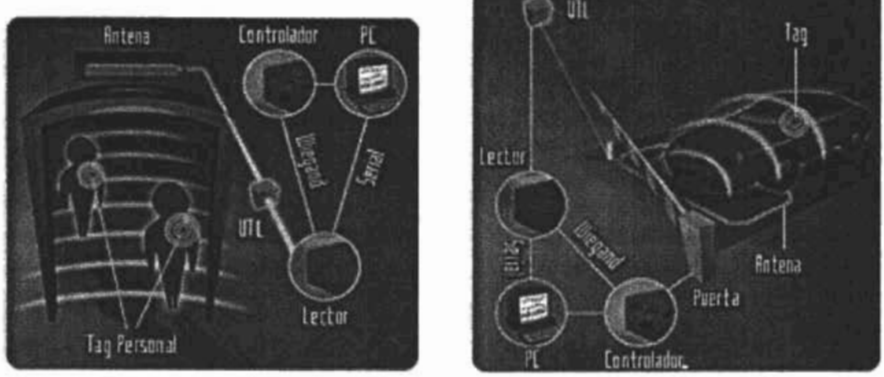


Figura 1.8 Aplicaciones de la radiofrecuencia

1.4 Tarjetas Inteligentes

1.4.1 Evolución de las Tarjetas Inteligentes

Las tarjetas desde hace varias décadas han transformado muchos procesos económicos, comerciales y sociales de ser humano.

Actividades que comúnmente realizamos involucran la utilización de estos dispositivos: transacciones monetarias, identificación de personas, transporte y teléfono público, control de acceso, comercio electrónico, telecomunicaciones móviles, son sólo algunos ejemplos de esta tecnología que ha ido evolucionando paulatinamente.

En sus orígenes la utilización de tarjetas vino a facilitar y simplificar el manejo de dinero en efectivo. En 1950 en Nueva York surge, como un medio de pago, la primer tarjeta de crédito llamada "Dinners Club"(Club de comidas) utilizada por hombres de negocios en diferentes restaurantes de la ciudad.

Debido a la portabilidad y comodidad que ofrecía esta tarjeta, propició una amplia difusión en el mercado mundial simplificando y automatizando muchas operaciones monetarias y comerciales. Su diseño basado en tecnología de banda magnética ofrece además un bajo costo por lo que su producción y adquisición por parte de diversas compañías crece considerablemente. Sin embargo se enfrenta a dos grandes desventajas su baja capacidad de almacenamiento y fraudes debido a una fácil reproducción de la misma.

Para resolver estos problemas se recurre a la búsqueda de nuevas tecnologías que procuren mecanismos de seguridad mucho más robustos y eficaces. La combinación de elementos tecnológicos tales como la microelectrónica y el procesamiento de datos dan origen a una nueva tecnología llamada "tarjeta inteligente". Es así como a finales de la década de los 70's se diseña la primer tarjeta inteligente por las compañías CII-Honeywell-BULL y Motorola, la cual portaba dos chips con la capacidad de almacenar una mayor cantidad de datos y procesar la información.

La complejidad de estos nuevos dispositivos ha ido creciendo a medida que surgen nuevas tecnologías y las necesidad de garantizar mucho mayor seguridad se vuelve un elemento indispensable de su constitución.

Para poder desarrollar adecuadamente una aplicación haciendo uso de esta tecnología es necesario entender que es una tarjeta inteligente, cual es su arquitectura y como opera.

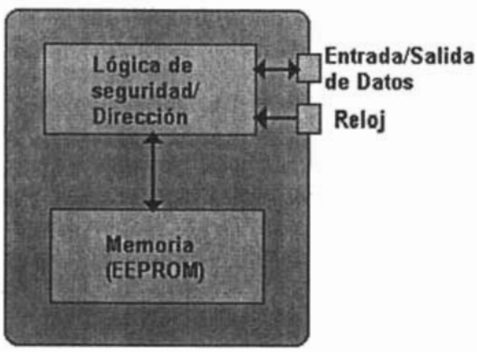
1.4.2 Definición de una tarjeta inteligente

Una tarjeta inteligente tiene una apariencia física muy similar a las tarjetas de crédito en cuanto a su tamaño y a su recubrimiento plástico, sin embargo están provistas por un circuito integrado el cuál le da su carácter "inteligente".

Su objetivo principal es el almacenamiento de información de una manera segura, confiable y en cierto aspecto autónoma. Su constitución además garantiza mayor resistencia a daños físicos externos e internos.

1.4.3 Tipo de Tarjetas

El estándar ISO 7816 define los parámetros físicos y lógicos de las tarjetas inteligente. Las funciones y características de las tarjetas depende fundamentalmente del tipo de circuito integrado y del método que se utilice para acceder a su información. Por lo que podemos encontrar tarjetas con memoria y con microprocesador; así mismo tarjetas de contacto y sin contacto.



Las tarjetas con memoria tienen una capacidad mucho mayor para guardar información. Actualmente encontramos tarjetas con una capacidad de almacenamiento de hasta 32 KB (equivalente a más de 32,000 caracteres), siendo su costo proporcional a la cantidad de información que pueden resguardar.

Figura1.9 Tarjetas con memoria

Para poder proteger la lectura y escritura de información, este tipo de dispositivos tienen la posibilidad de manejar distintos niveles de seguridad.

Las tarjetas pueden ser de sólo lectura, constituidas por una memoria cuyos datos pueden ser grabados una sola vez (PROM), su código de identificación generalmente es asignado en fábrica y no puede ser alterado; o bien tarjetas de lectura / escritura formadas por una memoria regravable (EEPROM) en donde la información puede ser modificada alrededor de 100, 000 veces.

Las etiquetas de identificación ó tarjetas con memoria, incluyen un identificador principal o número de serie, el cual es único, y la información que variará de acuerdo a la aplicación de la tarjeta por lo que algunas incluyen un contador lógico (en el caso de los monederos electrónicos o tarjetas telefónicas), datos y códigos secreto o llaves que pueden ser programadas para seguridad de la información.

Las tarjetas con microprocesador tienen integrado un microchip cuyas funciones son equivalentes al CPU (Unidad Central de Procesamiento) de una computadora, por lo que su capacidad va más allá de almacenar información, pueden además realizar operaciones internas y procesar la información que tienen almacenada. Esta cualidad expande su campo de aplicación, principalmente hacia aplicaciones que requieren la manipulación o comparación de datos.

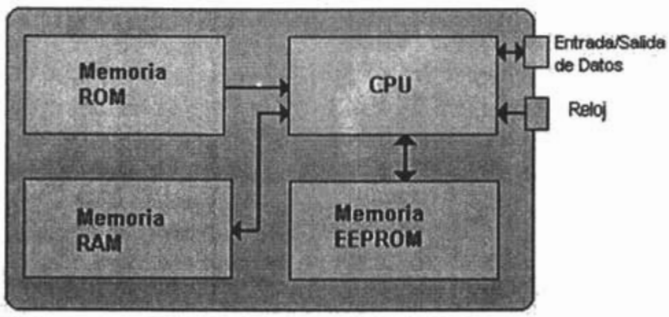


Figura 1.10 Tarjeta con microprocesador

Además de los circuitos electrónicos, la tarjeta con microprocesador posee un sistema operativo en el chip el cuál le permite operar las funciones internas propias de la aplicación, esta plataforma interna se almacena en una memoria de sólo lectura (ROM), similar a la que encontramos en el BIOS de una computadora.

Analizando la operatividad de una tarjeta con microprocesador podemos observar que su tecnología está basada sin duda en las computadoras modernas. Propiamente este dispositivo es reconocido como "inteligente" porque puede recibir información, procesarla y tomar decisiones.

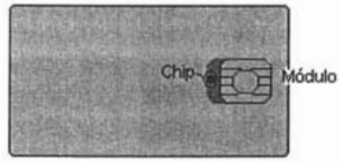


Figura 1.11 Tarjeta de contacto

Por la forma en que las tarjetas interactúan con el dispositivo lector se clasifican en tarjetas de contacto y sin contacto. Las tarjetas de contacto tienen que ser introducidas en el dispositivo lector, de manera que la unidad de entrada / salida del dispositivo se comunique con la terminal para transferir la información. Su arquitectura básica está diseñada a partir de un microchip enlazado a un módulo de contacto que interactúa directamente con la terminal o módulo lector. Entre los dispositivos más comúnmente utilizados tenemos las tarjetas de crédito y las tarjetas telefónicas.

Figura 1.12 Tarjeta sin contacto

Las tarjetas sin contacto están diseñadas bajo la tecnología de radiofrecuencia. Este tipo de dispositivos cuentan con una antena integrada para captar la información recibida a través de un campo electromagnético y un microchip que demodula y procesa los datos recibidos, así mismo es capaz de transmitir una respuesta a través de la antena para ser captada por la antena del dispositivo lector. Este tipo de sistemas han sido aceptados exitosamente debido a los grandes beneficios que ha aportado a muchas actividades del ser humano, como son control de acceso, protección de equipo, control de equipaje en los aeropuertos, control de ganado, control de procesos industriales, protección de vehículos, telecomunicaciones móviles (recientemente tecnología GSM), etc.

1.4.4 Ventajas de la tarjetas inteligentes

Las aplicaciones de las tarjetas inteligente han ido creciendo debido a las grandes ventajas que proporciona, principalmente:

- Una mayor seguridad. Los datos almacenados están protegidos por mecanismos de seguridad que parten de complejos programas de encriptación de acuerdo a la aplicación de la tarjeta. Por ello resulta muy difícil y costoso modificar los datos o falsificar las tarjetas.

- Rapidez. Las tarjetas inteligentes utilizadas para operaciones monetarias pueden realizar transacciones fuera de línea que generalmente tardan una fracción de segundo en comparación con los varios segundos que requieren las transacciones en línea. Las tarjetas sin contacto permiten transacciones aún más rápidas y cómodas para el usuario, permitiendo un ahorro significativo en costos y una mayor eficiencia.

- Capacidad de almacenamiento. Actualmente puede almacenar 100 veces más información que una tarjeta de banda magnética. Además de ofrecer la posibilidad de almacenar varios procesos en una sola tarjeta, permite realizar un sin fin de operaciones.

- Flexibilidad. La tarjeta inteligente tiene una amplio rango de aplicación, siendo utilizada en diversos ámbitos de la actividad humana.

- Portabilidad y comodidad para los usuarios.

La mayor ventaja es sin duda que está tecnología sigue creciendo de manera increíble, por lo que se encuentra en un mejoramiento continuo que garantiza cada día mejores resultados, y un mayor número de aplicaciones.

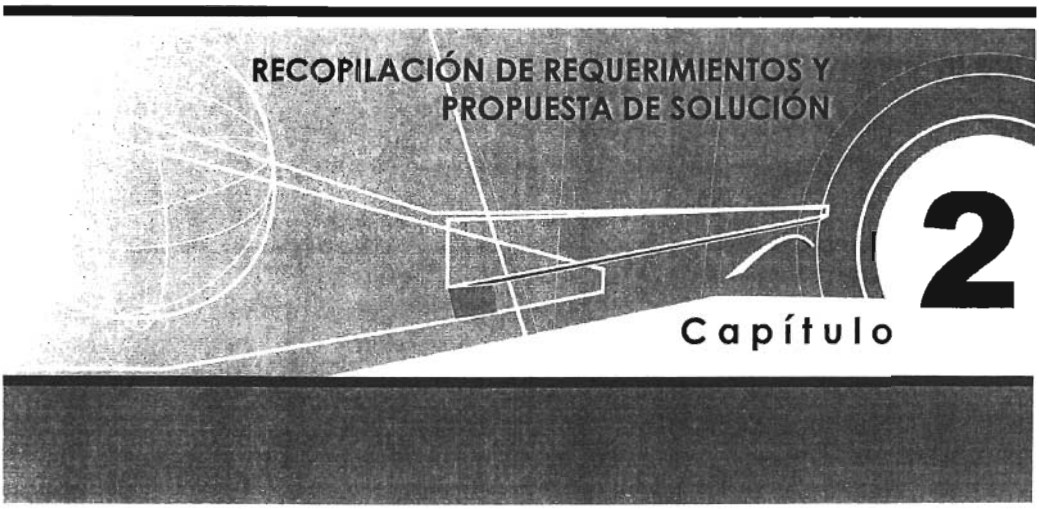
Figura 1.13 Aplicaciones de las tarjetas inteligentes

Actualmente nos encontramos inmersos en una sociedad donde el manejo de información y las comunicaciones ocupan la mayoría de las operaciones de negocios y de ámbito social. La necesidad de poder proteger los datos se ha convertido en algo imprescindible en nuestras vidas.

La búsqueda de soluciones que garanticen la seguridad de manera total no es posible si sólo nos enfocamos a cierta tecnología. Para desarrollar un sistema completo es imperativo que combinemos de manera audaz varias técnicas que nos permitan un mayor control de todas las situaciones que se nos puedan presentar.

De tal forma que tecnologías como la radiofrecuencia, las tarjetas inteligentes, la biometría puedan utilizarse de manera conjunta para generar sofisticados mecanismos de seguridad.

Es importante además contar con un soporte computacional que proporcione los antecedentes necesarios para la identificación efectiva del dispositivo y una lógica estructurada que pueda generar una acción de acuerdo a los datos recibidos.



RECOPILACIÓN DE REQUERIMIENTOS Y PROPUESTA DE SOLUCIÓN

Capítulo 2

Capítulo

2

RECOPILACIÓN DE REQUERIMIENTOS
Y PROPUESTA DE SOLUCIÓN

2.1 Antecedentes

La UNAM es una institución que esta encaminada a la formación y desarrollo académico, la investigación y la difusión de la ciencia y la cultura. Para poder lograr cumplir con tan loables objetivos, a parte de contar con un enorme capital humano, la universidad cuenta con recursos e instalaciones propios a las actividades que se desempeñan en cada una de las dependencias, escuelas, facultades e institutos que integran esta gran casa de estudios.

Los murales de la Rectoría y de la Biblioteca Central, el Telescopio de San Pedro Martir, el Palacio de Minería y el Palacio de Medicina son solamente algunos ejemplos que nos dan idea de lo invaluable que resulta el patrimonio universitario, no únicamente por su costo sino también por su contenido cultural, histórico o tecnológico, de interés tanto para la comunidad universitaria como para la nación.

Desafortunadamente por la dimensión, extensión y naturaleza pública de la mayoría de los espacios que integran la totalidad del patrimonio, a pesar de la conciencia que se tiene sobre su valía, el resguardo de instalaciones y personal ha resultado una tarea ardua y poco afortunada. Tan sólo en Ciudad Universitaria, a diario se registran un gran número de actos ilícitos que van desde daños a mobiliario, robo de equipos hasta daños mayores como son las pintas a murales , etc.

Todo lo anterior ha motivado a que las autoridades universitarias pongan especial énfasis a todo lo que se refiere a seguridad. De hecho la UNAM cuenta con una dependencia dedicada a proporcionar servicios de protección a personas y bienes dentro de las instalaciones universitarias: "La Dirección General de Servicios Generales". Mientras que las Escuelas y Facultades, cuentan con comisiones locales de seguridad.

El papel que desempeñan las Comisiones Locales es de gran importancia ya que al encontrarse inmersas en la problemática ofrecen soluciones concretas a problemas específicos. En respuesta a las necesidades particulares de cada espacio como son: ubicación y extensión de las instalaciones, horarios de trabajo, matrícula de estudiantes, etc.

En la Facultad de Ingeniería, la Comisión de Seguridad Local, ha tenido una difícil labor ya que en años recientes el número de actos ilícitos registrados en las instalaciones, se ha incrementado de manera considerable, en especial el robo.

Dicha situación es de impacto negativo para las grandes inversiones que anualmente se hacen en adquisiciones de equipo, al mismo tiempo que afecta el ambiente laboral y estudiantil provocando un clima de inseguridad y desconfianza. Además que la problemática se ve beneficiada en gran medida por la evidente falta de vigilancia en las instalaciones.

Por tal motivo, la búsqueda de soluciones factibles ha sido una tarea prioritaria para la institución y ha propiciado el surgimiento de diversos proyectos orientados a la seguridad.

Las diversas medidas posibles van desde un plan de contratación de nuevo personal de vigilancia, la instalación de cámaras de circuito cerrado, la adquisición de equipos de radiocomunicación hasta el uso de sofisticadas tecnologías de seguridad. Es precisamente dentro de uno de dichos proyectos que surge el presente trabajo de tesis.

Sin lugar a dudas todos los proyectos contemplados por la comisión local juegan un papel importante en el Plan de Seguridad de la Facultad, sin embargo en su gran mayoría únicamente ofrecen soluciones parciales a la problemática planteada, por ejemplo: La instalación de cámaras en diversas áreas. Aunque permite tener un registro de los actos delictivos, no implementa una acción contra el atentado y mucho menos lo evita. Por otra parte, el proyecto de contratación de nuevo personal de vigilancia se ve limitado por las restricciones económicas de la Universidad , donde por lo general es más probable un despido que la creación de nuevas plazas, etc.

En nuestro proyecto buscamos ofrecer una solución global. De tal manera que después de un análisis de las circunstancias que generan el problema principal se concluyo que la mejor opción radicaba en integrar distintos elementos en un Sistema de Seguridad diseñado a la medida con posibilidades de alcance incluso a nivel Facultad.

El proyecto se denomino "Tarjetas Inteligentes" y es un Sistema de Seguridad de última generación, es decir que no únicamente es capaz de detectar circunstancias anómalas, emitir una señal de aviso y efectuar alguna acción sino que también cuenta con "inteligencia" brindada por un soporte computacional que le permite decidir entre eventos, registrarlos e incluso llevar a cabo un control

totalmente autónomo únicamente requiriéndose una sencilla recopilación de datos de las características físicas de las instalaciones y requerimientos de seguridad.

El sistema emplea tecnología de radiofrecuencia para la implementación de zonas de acceso restringidas, por medio de una red de antenas, uso de dispositivos de transmisión y recepción de señales de radiofrecuencia que de aquí en adelante llamaremos "transponders" y tarjetas inteligentes para la identificación. Todo integrado a un servidor con software de control de eventos y comunicaciones además del soporte de una base de datos para registro.

El alcance de la tesis no incluye todo el sistema, sino más bien únicamente el análisis, diseño e implementación del software que se emplea como soporte computacional. En el presente capítulo, veremos de manera general un poco de las circunstancias y características que dieron forma al proyecto para poder entender ¿que dio origen? y ¿cuales son? los distintos usuarios y requerimientos.

2.2 El proyecto

2.2.1 "Tarjetas inteligentes"

La idea del proyecto surgió de un desarrollo local del Centro de Diseño y Manufactura de la Facultad de Ingeniería, donde un sistema similar demostró ser muy eficiente.

Hace 10 años se registró un robo en las instalaciones del Centro y desde ese entonces se tomo con mucha seriedad la búsqueda de alternativas en seguridad. A través de los años se probaron diversas opciones, comenzando por la más básica que fue la instalación de una segunda puerta además de la principal, pasando por diversas variaciones de cerraduras mecánicas y ya con los avances tecnológicos sistemas como el de acceso por identificación de código de barras. Sin embargo todas las opciones mostraron ineficiencia, incluso el sistema que parecía ser más eficaz. La detección por código de barras, con una vigencia de cuatro años, falló, cuando los estudiantes encontraron la forma de acceder al centro al replicar el código por medio de una copia impresa. Con cada anomalía presentada se buscaban mejoras en la tecnología empleada o la elección de nueva opción, así fue como se llegó a un último desarrollo, un proyecto llamado "Control de Acceso de Personal y de Tarjeta Inteligente" que actualmente se encuentra en operación.

"Control de Acceso de Personal y de Tarjeta Inteligente" es un sistema de control de acceso que emplea la tecnología de identificación por radiofrecuencia (RFID)[1] para proporcionar un acceso limitado a las instalaciones del CDM en base a la identificación de tarjetas especiales que únicamente portan el personal y estudiantes autorizados.

La credencial contiene un chip con un código de identificación único, dicho código es leído y enviado a una PC en el momento que el usuario acerca su credencial a la unidad lectora colocada en la puerta de entrada. La PC valida la información en una base de datos que contiene información de todo el personal del CDM y en base a ello concede o niega el acceso.

El identificador único en la Base de Datos esta relacionado con toda la información útil necesaria para permitir o denegar el acceso como: datos personales del usuario, horas y días de acceso autorizado, vigencia de la credencial, etc. Además de contar con registro histórico de todos los eventos ocurridos como todas las entradas y salidas de los usuarios por día, intentos de acceso no autorizados, etc.

El éxito operativo de esta primera experiencia, aunado a las múltiples ventajas de la tecnología de radiofrecuencia, como son :

- Que el principio operativo es sencillo como el de código de barras, pero más confiable y seguro.

- Que la identificación es discreta y sin muchas molestias para el usuario, debido a que no requiere contacto de el dispositivo de identificación con el lector.

- Que el uso de esta nueva tecnología es la pauta para nuevas aplicaciones como monederos electrónicos, transacciones de dinero e información mediante tarjetas inteligentes.

- Y que es un tecnología económica comparativamente con otros sistemas de identificación igual de eficientes como el reconocimiento de voz o huellas digitales.

Motivaron a que un sistema sobre la misma plataforma tecnológica "la radiofrecuencia" fuera propuesto y aceptado como solución factible a las necesidades de seguridad de la Facultad, dicho proyecto fue llamado "Tarjetas Inteligentes".

[1] (RFID) Radio Frecuency IDentification

2.2.2 Primeras consideraciones

Así el proyecto toma como base la configuración elemental de un sistema de identificación por radiofrecuencia formado por tres componentes elementales: lectores (readers), dispositivos emisores de radiofrecuencia (transpounders) y antenas. Más, nuevos elementos integrados en función a las necesidades planteadas por las autoridades de la Facultad quienes de manera esencial requerían:

- Garantizar al personal y estudiantes áreas seguras
- Proteger los bienes de la institución
- Proteger las instalaciones y evitar actos ílicitos

La protección de equipo y definición de áreas seguras es sencilla con los dispositivos de identificación del sistema, que son colocados en los equipos y portados por personal autorizado en forma de credencial para ser detectados por las antenas a la entrada de cada área cuando se intenta un acceso a las instalaciones o la salida de equipo.

Mientras que en la protección de instalaciones y prevención de actos ilícitos se considera el uso de nuevos elementos, dos clases distintas de dispositivos: sensores y actuadores. Los sensores permiten conocer el entorno que se esta resguardando, cualquier cambio en las condiciones normales de las instalaciones es detectado como un evento anómalo y la información es enviada al resto del sistema para posteriormente con los actuadores llevar a cabo alguna acción en específico.

2.2.3 El software

Ninguno de los componentes mencionados opera sólo. La información enviada por los transpounders através de las antenas a los lectores necesita forzosamente ser procesada para determinar si el acceso de personal y la salida de equipo es autorizada o no. Lo mismo que los datos recopilados por los sensores requieren procesarse para obtener la información que será enviada a los actuadores y traducida en acciones.

Desde este punto de vista, de forma estricta los dispositivos del sistema pueden ser vistos como entrada y salida de datos con un proceso intermedio. Hecho que justifica la integración de un último elemento al sistema; una PC con el software adecuado para efectuar los procesos necesarios con la información y agregar funcionalidades al sistema.

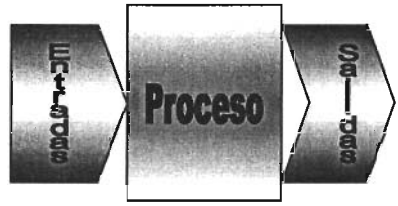


Figura 2.1 Proceso básico

De los anterior resulta evidente que en primera instancia lo que se espera de la aplicación es:

- Que se comunique con los dispositivos del sistema
- Que guarde la información a procesarse
- Que procese la información en una lógica de decisión que reconozca eventos y en base a ello seleccione una acción adecuada.

Además, la aplicación desde sus inicios se planteó sin perder de vista los alcances del proyecto, por tal motivo, con mira en las expectativas de llegar a tener un alcance a nivel Facultad , conjuntamente con las funciones básicas mencionadas se planteo una otra característica fundamental:

- Que el sistema sea fácil de modificarse para agregar nuevas funcionalidades, dar mantenimiento o adaptarse a diversas instalaciones

2.2.4 Integración con el hardware

Cuando se trata de tecnología de Radiofrecuencia existe en el mercado de la electrónica una amplia oferta de dispositivos entre los cuales es difícil elegir. Una adecuada elección se da en función de diversos parámetros entre otros: la disponibilidad de los dispositivos, el costo, la facilidad de configuración, instalación y operación, soporte técnico, que se trate de una tecnología abierta, etc.

En nuestro caso ésta delicada elección fue tarea de los compañeros encargados por la parte electrónica del proyecto que optaron por los dispositivos de Texas Instruments quién es líder mundial en esta área y cuenta con la más extensa variedad de dispositivos transmisores y lectores de radiofrecuencia.

La funciones esperadas en los dispositivos elegidos así como las necesidades expresadas por parte de los compañeros son de gran importancia en las consideraciones tomadas en cuenta para el diseño de la aplicación ya que como

se menciono en las primeras consideraciones los dispositivos necesitan de la intervención de la PC para su funcionamiento.

Estrictamente los elementos que componen el sistema se integran en tres subsistemas según su aplicación:

- Sistema de control de acceso
- Sistema de protección de equipos
- Sistema de alarmas contra intrusos

Sistema de control de acceso

El sistema de control de acceso garantiza al personal y estudiantes áreas seguras ya que ofrece una forma de tener dominio sobre el flujo de entrada y salida de personas a determinadas instalaciones y de esta forma evita la entrada de personas no deseadas como podría ser el caso de un maleante. Para tal propósito se propuso el uso de credenciales personalizadas para la identificación. Cada credencial contiene la fotografía, el nombre y el cargo del portador y un chip con un número de identificación que será leído por un lector colocado en los accesos de las instalaciones a resguardar. La información del lector es validada en base a la hora,día y área que se pretende el acceso y dependiendo del resultado de la validación se permite o niega el acceso.

Sistema de Protección de Equipos

Este sistema evita los robos en las instalaciones resguardadas mediante la colocación de un transponder en los bienes que se consideren valiosos. Los equipos protegidos únicamente pueden salir de las instalaciones previa autorización de el responsable del equipo.

Sistema de alarma contra intrusos

Típicamente cuando un intruso pretende cometer algún acto ilícito al escuchar una alarma prefiere retirarse antes de ser atrapado. De ahí la mayor útilidad de colocar un sistema de alarmas que de una señal sonora en respuesta a eventos específicos. Las alarmas se activan en base a la información enviada por distintos tipos de sensores que se propone colocar en áreas estratégicas de las instalaciones.

Los sensores que propone colocar son de tres tipos:

- Sensores de movimiento
- Sensores magnéticos

- Sensores de ruptura

Los sensores de movimiento son para detectar la entrada de intrusos en las instalaciones, estos estarán activados únicamente cuando no haya nadie en las instalaciones a proteger.

Los sensores magnéticos son para detectar cuando una puerta se encuentra abierta y cerrarla. De esta forma evitar que personas que no cuentan con credencial tengan acceso.

Por último los sensores de ruptura son para detectar cualquier intento de entrada en las instalaciones a través de ventanas. Estos sensores estarán activos las 24 horas del día.

Cada subsistema como ya se menciono depende del control maestro que es la PC entonces cada una de las funciones mencionadas se traducen en características necesarias en la aplicación a diseñar. Así el software debe ser capaz de:

- Validar información de identificación de personal
- Validar la información de identificación de equipo
- Autorizar/Denegar entradas y salidas de personal
- Autorizar/Denegar salidas de equipo
- Activar/desactivar alarmas
- Abrir/cerrar puertas de las instalaciones
- Activar/Desactivar dispositivos
- Registrar todas la acciones efectuadas por el sistema
- Registrar todos los eventos detectados por el sistema

Además como para poder lograr todo lo anterior la aplicación primero debe contar con los dispositivos, la aplicación requiere:

- Añadir/ Eliminar dispositivos fácilmente
- Configurar lógica interna de los dispositivos
- Configurar lógica de acción de los dispositivos

Pero nada de lo anterior importa si no se cuenta con una adecuada comunicación por ello también debe cumplir con los requerimientos técnicos:

- Comunicarse a través de puerto serie de la PC
- Emplear el protocolo de comunicación que ocupan los dispositivos
- Respetar las velocidades de transmisión y recepción de los dispositivos

En cuanto a las necesidades expresadas por parte de los compañeros encargados de la parte electrónica destaca:

- Contar con una interfaz secilla y de fácil uso para la administración de dispositivos

2.2.3 Los usuarios

La Facultad de Ingeniería actualmente cuenta con 70 personas asignadas como personal de vigilancia cantidad que resulta minúscula en contraste con las grandes cifras manejadas en inventarios de equipo e inmobiliario. De hecho las instalaciones son consideradas entre las más extensas del campo universitario: con 4 bibliotecas, 4 auditorios, 9 salas de computo, 78 laboratorios y 23 edificios por lo que es casi imposible contar con un adecuado resguardo.

Por tal motivó una de las principales consideraciones del diseño del software fue garantizar un manejo casi autónomo del sistema con la mínima intervención humana. Así que funciones básicas como la comunicación con el hardware para la detección de equipo, acceso de personal y el registro de eventos en la base de datos se hacen de manera automática siendo únicamente las operaciones de configuración inicial del software, mantenimiento a la base de datos y nuevo hardware las que requieren de interacción con personal. Lo anterior derivo en la necesidad de que el software a desarrollar tuviera la robustez de un servidor para poder ejecutar procesos permanentes al mismo tiempo que atiende peticiones externas.

Desde este punto de vista, el sistema entre otros objetivos se propone ser un apoyo al personal de vigilancia y no una carga más a sus ya múltiples responsabilidades. Sin embargo como la mayoría del personal de vigilancia son mujeres o hombres de edad avanzada o jóvenes con escasos o nulos conocimientos en cómputo se consideró una mejor opción como usuarios directos del sistema al personal administrativo y/o acádemico mientras que el personal de vigilancia únicamente es el punto de acción final en caso de algún acto ílicito.

Diseñar el software para el personal administrativo y/o académico provee algunas ventajas al sistema. En primera instancia el tiempo de capacitación en el manejo del software se reduce mucho en términos comparativos con el tiempo que tomaría entrenar al personal de vigilancia ya que normalmente el personal académico y administrativo se encuentra habituado al manejo de distintos programas de computo y el manejo de uno nuevo no implicaría mayor complicación que una corta capacitación o una sencilla consulta a los manuales. Además que quien mejor para administrar el software y tomar decisiones sobre configuración e instalación de dispositivos que el personal que conoce a la perfección las labores cotidianas, instalaciones y valores a proteger.

Quizás el único inconveniente de esta decisión es que el personal designado para la operación del software se distrae de sus actividades cotidianas. Aunque la

distracción es realmente poca debido a que como ya se menciono uno objetivo perseguidos con el software es la autonomía se decidio implementar otras dos medidas

Como ya se mencionó la interacción con el software no es constante sin embargo en los casos que es necesaria es de gran impacto para el resto del sistema de ahí la importancia de decidir los distintos niveles de iteracción por

- Quien mejor que el mismo personal que labora en el sitio a proteger conoce las condiciones normales de trabajo, las instalaciones, las condiciones de riesgo y los valores a salvaguardar para proveer de información al software y que este opere de manera óptima.

2.2.4 Lugar de la instalación del Sistema

Finalmente se decidió que el sistema sería instalado en un edificio de la Facultad. Para este punto los requerimientos recopilados hasta el momento para el software ya convergían en una estructura con completa funcionalidad y fácil adaptación a casi cualquier instalación donde fuera destinado, sin embargo la información obtenida del lugar específico de instalación fue básica para terminar de dar forma al software. Ya que fue hasta este momento; resultado de observar las instalaciones, la forma de trabajo del departamento y observaciones directas del personal, que logramos aterrizar algunas de las características funcionales que aunque ya habían sido contempladas no contaba con parámetros reales para el desempeño, además de agregar nuevas consideraciones que contribuyeron a la mejora del diseño de la aplicación propuesta.

En el lugar a instalar la principal actividad es la docencia aunada a labores de investigación básica y aplicada, intercambio académico y asesoría a organismos públicos y privados todo con el fin de apoyar en la mayor medida el proceso de enseñanza aprendizaje. Para efectuar dichas actividades cuenta con diversos recursos materiales:

- Oficinas: Donde el Jefe del Departamento, los profesores de carrera de tiempo completo, los coordinadores de laboratorio y el resto del personal administrativo y acádemico cuentan con todo los materiales y equipo necesario para efectuar sus actividades cotidianas.

- Laboratorio de Máquinas Térmicas. Este laboratorio cuenta con instalaciones de tipo industrial de baja capacidad para el desarrollo de pruebas convencionales en diversos equipos térmicos tales como turbinas de gas y vapor, compresores, motores de combustion interna, calderas e intercambiadores de calor, entre otros.

- Laboratorio de Termofluidos. El Laboratorio de Termofluidos cuenta con el equipo especialmente diseñado para llevar a cabo los experimentos básicos de los cursos de Mecánica y Dinámica de Fluidos, Turbomaquinaria, Máquinas de Desplazamiento Positivo y Transferencia de Calor.

- Laboratorio de Control de Emisiones. El Laboratorio de Control de Emisiones tiene como objetivo principal desarrollar proyectos de desarrollo e innovación tecnológica en el área de emisiones, particularmente aquellas provenientes de los motores de combustián interna. En la actualidad cuenta con un banco de pruebas estacionario para motores, un banco de rodillos para pruebas de vehículos y un banco de rodillos para pruebas de motocicletas.

- Laboratorio de Investigación. Las instalaciones del Laboratorio de Investigación tienen como objetivo principal el poder llevar a cabo los proyectos de investigación básica y aplicada que sirvan para lograr una aportación al conocimiento en las área de Mecánica de Fluidos y de Ingeniería Térmica, teniendo como productos asociados tesis de licenciatura y posgrado. Para el desarrollo de tales actividades, el Laboratorio cuenta con un banco de flujo, un anemómetro de hilo caliente, un anemómetro laser de efecto Doppler de dos canales, dos anemómetros laser de efecto Doppler de un canal y equipos electrónicos diversos de medición.

De tal cantidad de recursos y en especial del hecho de que muchos de ellos sean de costos elevados no resulta extraño que este edificio haya sido elegido como punto de partida para el sistema.

Una vez conocidas las instalaciones a salvaguardar por lo que respecta al hardware, los compañeros encargados por la parte electrónica del sistema en conjunto con el personal de termoenergía delimitaron las áreas de acceso restringido y definieron la ubicación estratégica de puertas, antenas y cerraduras así como de los dispositivos sensores y actuadores. Mientras en lo que respecta al software el punto focal fue mejorar el diseño de tal manera que el software fuera capaz de implementar la estrategia de seguridad adecuada al Departamento de Termoenergía respetando al máximo las actividades normales del Departamento.

Entre la información detectada que tuvo un impacto en el diseño del software destaca:

- El personal de Termoenergía trabaja de Lunes a Viernes en horarios normales de 8:00 a 21:00 horas pero en algunos casos se necesita también permitir el ingreso los fines de semana a determinadas áreas. Esta situación redundo en la necesidad de extender las consideraciones de

flexibilidad proporcionadas por el software para el manejo de horarios y dispositivos. Respectivamente, los horarios se extendieron a 24hrs con una semana laboral de 7 días y no de cinco como se había considerado y en cuanto a los dispositivos se considero un requerimiento que cada uno pudiera programarse de manera individual . De esta forma por ejemplo si alguien autorizado requiere entrar en fin de semana a determinada área únicamente los dispositivos sensores de dicha área serán desactivados en el día y hora que se espera el ingreso mientras que el resto del edificio será sensado normalmente.

En general adecuar una estrategia de seguridad a la forma de trabajo del Departamento se resume en que el software debe contar con una lógica de acción basada en parámetros flexibles, de fácil modificación e independiente del resto del sistema para poder efectuar cambios sin afectar al resto del sistema.

2.2.5 Seguridad del Sistema

A pesar de que la interacción de personal con el software no es constante en los casos que es necesaria tiene un gran impacto en el resto del sistema, de tal forma que quien tiene acceso al software podría hacer cosas como permitir que equipo salga de las instalaciones sin ser activado una alarma, decidir quienes pueden entrar a determinada área y en que horarios o mejor aún agregar nuevo harware o desactivar todo el sistema de ahí que un requerimiento más sea:

- El software debe ser seguro, de tal forma que no cualquier persona pueda accesar a todas las capacidades del sistema sólo personal responsable.

Así la aplicación maneja distintos niveles de acceso y manejo de información basandose en un esquema con tres distintos tipos de usuarios según su capacidades de acceso a la información:

- Administrador
- Usuario Avanzado
- Usuario normal

Administrador: Puede ver información de todos el sistema, su funcionamiento y hacer cualquier cambio.

Usuario Avanzado: Puede ver información de todo el sistema y puede manipular dicha infomación pero de manera limitada

Usuario Normal: Observa de manera parcial la información del sistema.

2.2.6 Resumen de especificaciones

En base a todo lo anteriormente mencionado las especificaciones de las funciones del software son las siguientes:

- Registrar E/S

  Personal
  - Hora entrada
  - Hora Salida
  - Fecha
  - Persona
  - Area a la que accesa
  - Número de veces que entró y salió.

  Equipo
  - Identificación de Equipo
  - Fecha de salida
  - Hora de salida
  - Departamento al que pertenece
  - Persona que lo está sacando
  - Quién lo autoriza
  - Tiempo de autorización

- Autorización de E/S

  Personal y Equipo
  - Horarios permitidos de entrada (para el personal)
  - Horario permitida de salida (para el equipo)
  - Fechas
  - Días permitidos.
  - Intervalos de fecha.

- Despliegue de avisos de eventos irregulares

  - Intento de acceso sin autorización (por horario no permitido, por fecha)
  - Entradas y salidas continuas
  - Activación de alarma por intento de robo de equipo
  - Exipiración del equipo de salida

- Que sea configurable

  - Poder configurar la cantidad de dispositivos que estarán conectados al sistema.
  - Poder configurar el número de puerto por donde se manejará la información.
  - Interrupciones que manejas el micro.

- Que maneje diferentes privilegios de usuarios para acceder al sistema.

  - Administrador. Todos los privilegios
  - Usuarios Avanzados. Algunos privilegios de administrador
  - Usuarios Restringidos. Consultas y desactivar alarma.

- Que sea seguro.

  - No cualquiera pueda cerrar el programa
  - Que tenga accesos restringidos según sea tipo de usuario.
  - Que maneje distintas interfases para los usuarios del sistema.

- Que almacene las entradas y salidas

  - Registro cotidiano de entradas y salidas del personal.
  - Que permita hacer respaldos de los registros
  - Registros de entrada y salida de equipo
  - Registros de eventos irregulares
  - Respaldo de los eventos irregulares

- Que evite el robo de equipo

  - Que detecte equipo y persona que salen de las instalaciones
  - Hora de salida del equipo
  - Que implemente un aviso del evento
  - Fecha de salida
  - Activación de alarma sonora y visual en caso de intento de robo
  - Que registre la hora y fecha de la activación de la alarma
  - Que registre hora en que se desactive y persona
  - Que cierre la salida principal en caso de intento de robo

- Que considere contingencias naturales e imprevistos.
  -
  - Fallas eléctricas (cortos circuitos)
  - Perdida de comunicación con las antenas.
  - Registro de la contingencia.

2.3 Propuesta de solución

2.3.1 Diseño modular

El software será diseñado por módulos perfectamente delimitados, cada módulo abarca específicamente sólo alguna de las capacidades del programa, esto para permitir el fácil crecimiento de la aplicación así como su fácil manejo. Los módulos son:

- Módulo de comunicaciones
- Módulo de Base de Datos
- Interfaz Principal
- Seguridad

Módulo de comunicaciones

En el modulo de comunicaciones se podrá Interactuar directamente con el hardware conectado a la aplicación desde donde se podrá hacer la configuración, mantenimiento, revisión de estado y detección de fallas de los dispositivos del sistema. La administración de los dispositivos abarca tres acciones sencillas:

- Agregar dispositivos
- Modificar dispositivos
- Eliminar dispositivos

Módulo de Base de Datos

Este modulo es el que realizara todas las funciones propias de mantenimiento y administración de la base de datos que contiene toda la información que procesa el sistema: datos de usuarios, equipos, incidentes, Entrada y Salida de Usuarios y salidas de equipo, etc. Las funciones básicas de la base de datos son:

- Validar la información para el acceso de personal y salida de equipo.
- Consultar, modificar o eliminar registros de personal, equipo o incidentes
- Guardar registros históricos de todo lo ocurrido

Interfaz Principal

Permitirá el acceso al resto de los módulos y el manejo sencillo de la aplicación.

2.3.2 Versión servidor

Además del diseño modular, proponemos que la aplicación operre como una versión Servidor con las siguientes características:

- Autonomía de operación
- Seguridad
- Y niveles de usuarios

Autonomía de operación

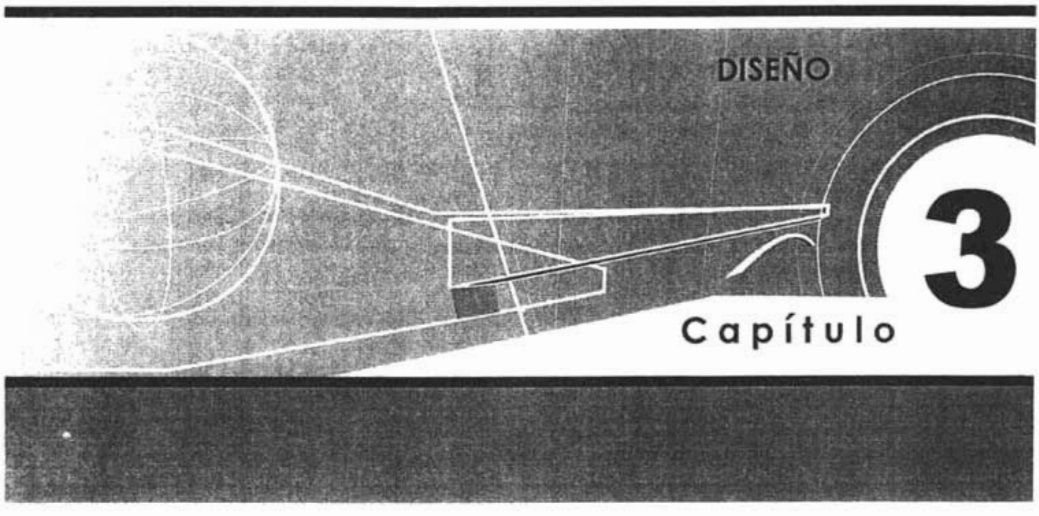
El software mantiene el proceso principal "Monitoreo de entrada de usuarios y salida de equipos" siempre activo, sin necesidad de ninguna supervisión adicional. Sólo en casos fuera de la operación normal como por ejemplo agregar nuevos dispositivos, activación de alarmas, etc. se requiere de la presencia de algún administrador.

Seguridad

No cualquier persona tiene acceso al sistema, únicamente quienes han sido registrados como usuarios. Para ello se propone un esquema de autenticación de accesos a través de una clave y contraseña.

Niveles de usuarios

Además de que no cualquier persona tenga acceso al sistema, se propone un esquema de niveles de usuarios de tal forma que según el tipo de usuario que se trate se tenga acceso únicamente a una parte de las funcionalidades del sistema. Un administrador contará con el acceso a todos los módulos en su total funcionalidad, seguido de un usuario avanzado, que tiene acceso a toda la información pero no capacidad para efectuar ninguna clase de modificación sobre lo que ve y finalmente un usuario restringido quien únicamente ve parcialmente la información arrojada por el software.


DISEÑO
3
Capítulo

Capítulo

3

DISEÑO

3.1 Diseño General

Una vez que realizamos la definición de requerimientos podemos proceder a realizar el diseño del software: "Sistema de Acceso a Personal y Protección de Equipo o SAPPE".

La complejidad del sistema completo y las restricciones tan particulares que debían cubrirse dieron la pauta para que organizáramos el programa de manera descendente, es decir la realización de subprogramas que cubrieran los intereses de todos los usuarios involucrados, facilitando no sólo su programación sino su mantenimiento y expansión. Por ello se consideraron cuatro módulos principales a partir de los cuales buscamos cubrir todas las expectativas definidas durante el análisis:

- Interfaz de Usuario
- Base de Datos
- Comunicaciones
- Seguridad

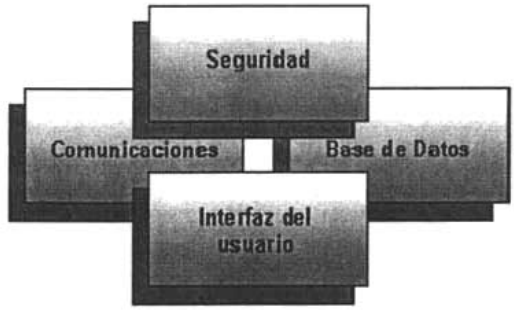


Figura 3.1 Módulos de SAPPE

El principal objetivo de diseñar el programa de manera modular fue debido a que se deseaba obtener un sistema funcional que pudiera ser fácilmente adaptado a otras instalaciones de la Facultad de Ingeniería, asimismo al ser parte de un sistema también es indispensable proporcionar un programa robusto y con el potencial para crecer adecuadamente con la aparición de nuevas tecnologías. Por otra parte las necesidades particulares de los distintos usuarios delimitaron el sistema en dos visiones: por un lado el personal interesado en la administración

de la información, del personal y del equipo y por otro lado los usuarios interesados en la administración y control del sistema físico de seguridad. El sistema desglosado se muestra a continuación. A partir de este diseño describiremos la estructura de cada uno de los módulos.

3.2 Comunicaciones

El módulo de comunicaciones es el enlace directo entre el hardware y el software, así como el punto crítico para el óptimo funcionamiento del Sistema de Seguridad por lo que su diseño y desarrollo absorbió la mayor parte del tiempo de programación de SAPPE, debido a su complejidad la generación de éste módulo implicó varias etapas de diseño y reestructuración para obtener una aplicación completa y eficiente que cubriera todas las expectativas del sistema. A continuación detallaremos el progreso evolutivo que sufrió la parte de comunicaciones a lo largo del proyecto.

3.2.1 Primer prototipo

El primer prototipo que se diseñó fue básicamente para verificar la forma en que nos comunicaríamos con el hardware. Como en todo sistema de comunicaciones existe un transmisor y un receptor, así como un medio de transmisión, en nuestro caso particular tenemos un sistema bidireccional de comunicación, es decir, la computadora es un transmisor y receptor a la vez. Por lo tanto en nuestro módulo consideramos los siguientes submódulos que ejecutarían el proceso de comunicación:

1. Interfaz de Comunicaciones
2. Submódulo de Tranmisión
3. Submódulo de Recepción

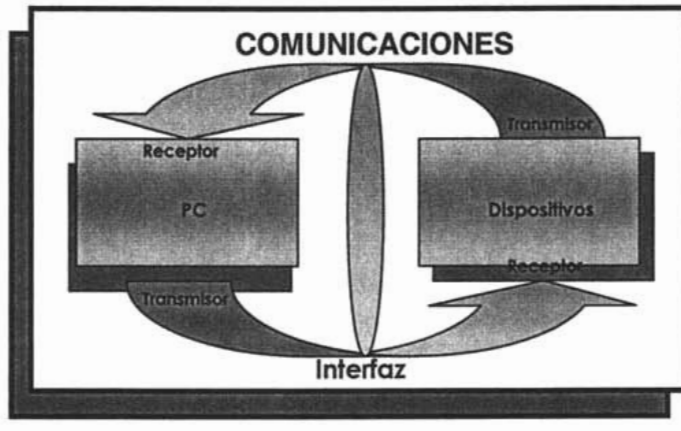


Figura 3.2 Primer prototipo: Comunicaciones

Submódulo de Interfaz de Comunicaciones

El módulo de Interfaz de comunicaciones tiene que ver directamente con la conexión física entre la computadora y el hardware, la comunicación se realiza a través del puerto serie por lo que se requiere una parte de software que manipule directamente la configuración del puerto.

Submódulo de Tranmisión

El módulo de transmisión contempla desde la formulación del mensaje que será enviado al hardware, el cálculo de un código de detección de errores para prevenir la corrupción del mensaje y la codificación del mensaje de manera que la cadena enviada corresponda con los parámetros utilizados por el protocolo de comunicación.

Figura 3.3 Comunicaciones: Proceso de Transmisión

Submódulo de Recepción

El hardware únicamente responde cuando enviamos una instrucción por lo tanto el proceso de recepción de datos es lineal al proceso de transmisión. El proceso de recepción de los datos involucra básicamente tres pasos al igual que en la transmisión, por un lado la decodificación de la cadena recibida de manera que podamos interpretarla, posteriormente decomponer la cadena para obtener los datos importantes y finalmente aplicarle un método de detección de errores para verificar que el mensaje haya llegado correctamente.

Figura 3.4 Comunicaciones: Proceso de Recepción

Este primer diseño contempló los elementos básicos para establecer un sistema de comunicación con el hardware, el proceso de comunicación parte de la premisa de que la computadora controla la trasmisión de la información de manera que el hardware se mantiene como receptor a menos que la computadora le envíe una instrucción, esta última acción tiene como efecto una respuesta del hardware hacia la computadora. Para clarificar el proceso de comunicación se muestra a un diagrama de flujo (ver anexo A Fig. 1)

3.2.2 Segundo Prototipo

A partir del diseño básico del sistema de comunicaciones logramos establecer con éxito la comunicación entre el hardware y la computadora lo que nos dio la pauta para continuar con un diseño muchos más elaborado que tuviera la capacidad para actuar de manera autónoma respondiendo lógicamente a situaciones externas previamente establecidas.

Este nuevo diseño implicó establecer los procedimientos de operación del sistema de manera que el software tuviera la capacidad de tomar decisiones ante la información recibida y ejecutar las rutinas de seguridad correspondientes.

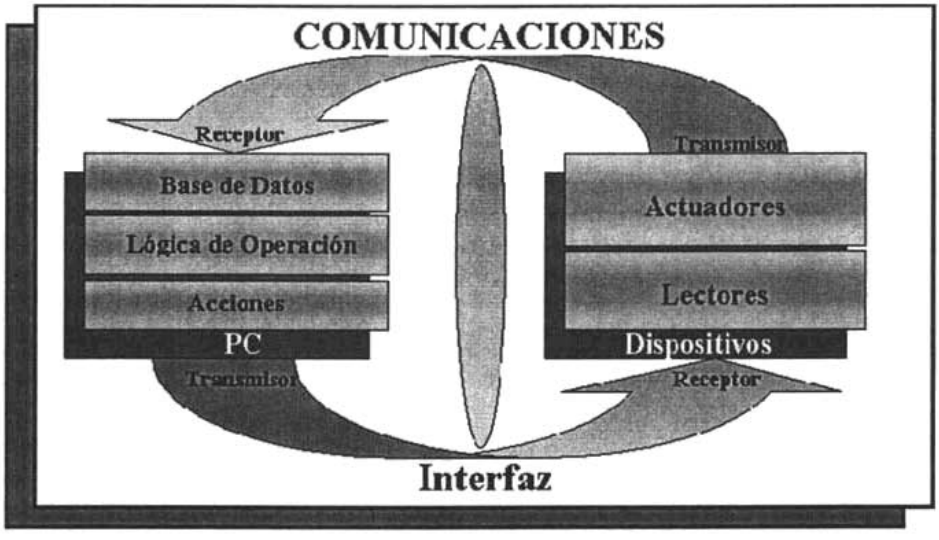


Figura 3.5 Segundo Prototipo: Comunicaciones

Una vez definidos los objetivos de nuestro sistema de seguridad el diseño involucró, como podemos ver en el diagrama anterior, la integración de nuevos elementos que contemplaran por un lado la protección física mediante hardware

y por otra parte una estrategia de seguridad que controlara la operatividad de los dispositivos.

Por la parte del hardware contamos con dispositivos lectores los cuales se encargan de identificar el acceso o salida de bienes y personal así como con actuadores, dispositivos controlables en forma eléctrica (tal como alarmas, chapas electrónicas, etc.) que llevan a cabo las acciones preestablecidas en nuestro plan de seguridad.

El software se diseñó con tres procedimientos adicionales: la comparación de los datos recibidos contra la Base de Datos, un proceso de evaluación de los datos obtenidos mediante una lógica de operación y finalmente la determinación de las acciones de emergencia para que puedan ser ejecutadas por los actuadores.

De esta forma el sistema completo quedó estructurado de la siguiente manera (ver anexo A Figura 2) :

1. Petición al dispositivo lector de la información capturada por éste.
2. Recepción del Mensaje.
3. Descomposición del Mensaje. (Identificador + Código de Detección de Error).
4. Comprobación del Mensaje Recibido.
5. Comparación del Identificador contra la Base de Datos.
6. Evaluación de la información obtenida mediante la lógica de operación.
7. Acción a seguir de acuerdo a la lógica de operación.
8. Formulación de la instrucción
9. Transmisión de la instrucción

Lógica de Operación

La primer estrategia de seguridad que diseñamos se enfocó a la protección del personal así como de los bienes involucrados mediante el control de acceso. Por lo tanto la estrategia se dividió en dos funciones principales: control de accesos y salidas de personal y control de salida de equipo. (Anexo A Figura 3) .

Evolución del segundo prototipo

Este sistema cubría las necesidades principales de seguridad, sin embargo no cumplía aún con todas las expectativas del proyecto. Se deseaba obtener un sistema mucho más completo y robusto que permitiera un crecimiento paulatino de las estrategias de seguridad. Asimismo se requería un sistema mucho más flexible que alojara la posibilidad de adaptarse a nuevas tecnologías, permitiendo la interconexión de sistemas electrónicos de detección, cámaras, etc.

Para poder establecer un nuevo modelo recurrimos a un análisis de las deficiencias y limitaciones del sistema para sustituirlas por funciones más adecuadas, conservando únicamente la infraestructura básica del sistema de comunicaciones.

En primer lugar consideramos que el diseño estaba contemplado para un número determinado de dispositivos, es decir si deseábamos agregar nuevos dispositivos forzosamente tendríamos que modificar el código del programa, lo que resultaba sumamente ineficiente. Para ello definimos los elementos del hardware para el Edificio, de manera que pudieran ser divididos en procesos independientes facilitando en un futuro la adición de otros tipo de dipositivos.

Estructura del Hardware del sistema

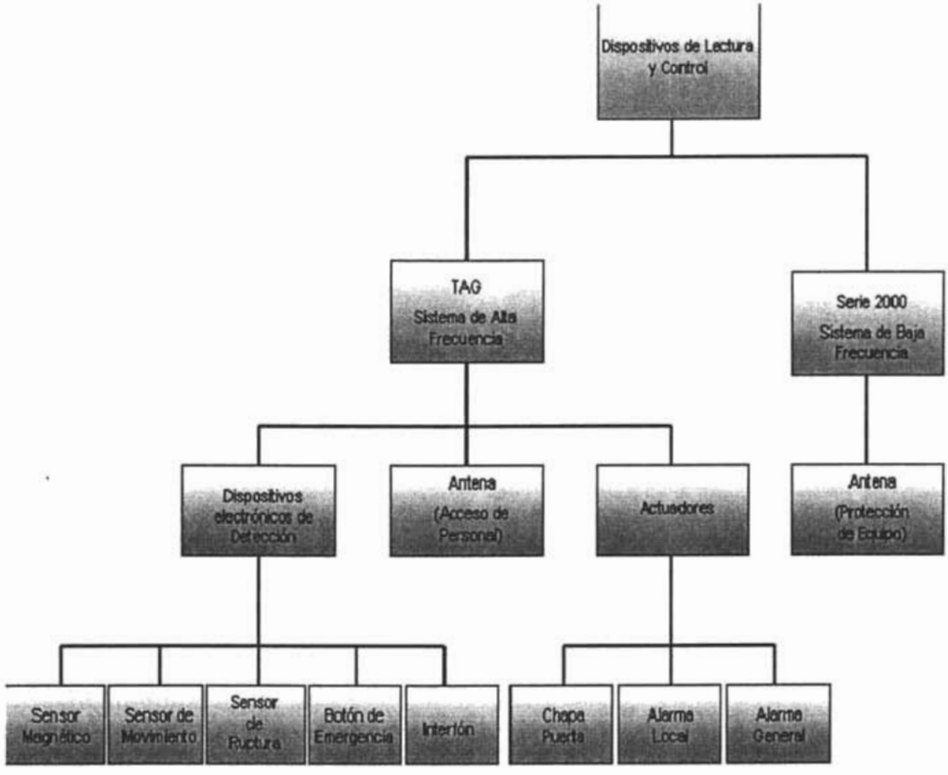


Figura 3.6 Estructura del Hardware del Sistema

Como resultado de esta fragmentación del hardware se requería una función que permitiera generar instrucciones de control específicas por cada dispositivo de acuerdo a sus características. Por lo tanto, con el apoyo de los compañeros de la sección de electrónica, definimos los comandos de operación por cada tipo de dispositivo de tal forma que nos permitieran obtener una secuencia lógica para la generación automática de instrucciones. (Ver Anexo A Figura 4)

Asimismo las especificaciones de los requerimientos del sistema con respecto al hardware demandaban restricciones particulares para cada tipo de dispositivo electrónico. La lógica del sistema, en consecuencia, debía agregar nuevos lineamientos de seguridad que consideraran los elementos de hardware adicionales. (Ver Anexo A Figura 5 y 6)

Finalmente consideramos que el sistema varía dependiendo de la necesidad de cobertura de acceso y de las zonas estratégicas de seguridad para cada edificio, por lo tanto definimos un sistema que permitiera la configuración de zonas críticas, lo que nos proporcionaría un sistema a la medida, pero con la capacidad para adaptarse fácilmente a otras instalaciones. De acuerdo a la arquitectura y distribución del edificio consideramos cuatro áreas vulnerables para el control de acceso del personal y protección de equipo.

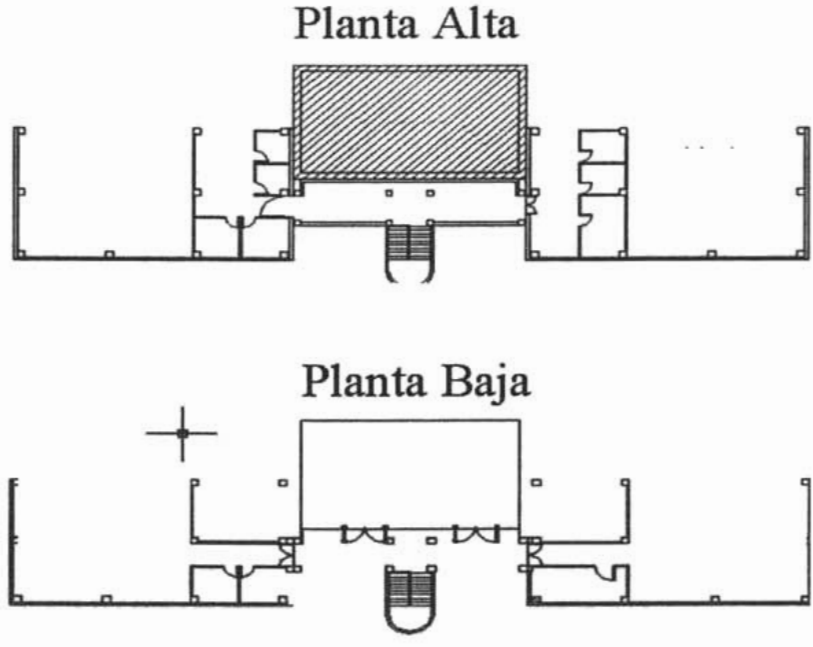


Figura 3.7 Zonas estratégicas de seguridad

Integración del software y el hardware

Una parte fundamental para el correcto funcionamiento del sistema es garantizar a través del flujo de información una sincronización total entre en hardware y el software en tiempo real. Para ello se requiere diseñar un sistema que permita configurar los tiempos de transmisión y recepción de manera asíncrona y aseverar en todo momento que no se pierda la comunicación bidireccional.

Las características de las cuáles partimos para lograr consistencia en la transmisión y recepción de la información fue que el hardware siempre responde ante cualquier petición por parte del software, así mismo el tiempo de respuesta por parte de los dispositivos no es igual debido a variables físicas como distancia, la naturaleza de los actuares y características del cable que afectan directamente la propagación de los datos.

Por otra parte al ser un sistema de seguridad los tiempos para ejecutar las acciones de emergencia determinadas se vuelven una parte crítica que exige invariablemente un proceso que optimice la comunicación entre el hardware y el software.

Dentro de los procesos involucrados en el sistema de comunicación debemos considerar tres tiempos importantes de los cuales va a depender la eficiencia y optimización del sistema total. Por lo tanto tendremos tres procesos principales: transmisión, recepción y respuesta con su tiempo respectivo de operación como se muestra en el siguiente diagrama.

Figura 3.8 Procesos principales en el sistema de comunicación

El proceso de recepción de datos será un importante detector de fallas en el hardware, debido a que podremos verificar si los dispositivos están o no respondiendo en el tiempo determinado.

Para unir la computadora con el hardware también fue importante definir el soporte físico que permitiría la propagación de los datos, debido a las distancias a las que sería implantado el sistema físico de seguridad. Por lo que fue importante buscar un cable que permitiera una alta velocidad de transmisión a grandes distancias, con el menor riesgo de distorsión y pérdida de información.

De antemano se había establecido la comunicación por puerto serial, para la cual se utiliza la conexión RS-232. Este tipo de unión permite transmisiones asíncronas y síncronas a gran velocidad, sin embargo su rendimiento sólo tolera cortas distancias.

Debido a esta limitante se decidió la combinación de otro tipo de unión que soportara grandes distancias: RS-485, conexión que permite la transmisión en entornos con ruido a distancias importantes. Además de que una comunicación RS232 es una conexión punto a punto mientras que una conexión RS-485 es punto-multipunto que permite conectar un número mayor de dispositivos.

3.3 Base de Datos

El módulo de base de datos es el encargado de ingresar, almacenar, procesar y proveer la información requerida por el resto del sistema. Es la principal fuente de información de la aplicación, de ahí su importancia, ya que la mayor parte de las funciones que se espera efectúe SAPPE están sujetas a los datos provenientes de este módulo.

Estrictamente el módulo es únicamente el elemento al interior de SAPPE que se conecta a Base de Datos, obtiene y manipula información. Pero, precisamente por las funciones que desempeña implica otros dos elementos: Base de Datos y el Sistema Gestor de Base de Datos, que aunque son externos a la aplicación, son indispensables. En la figura 3.x se observa como se integra el módulo en el sistema:

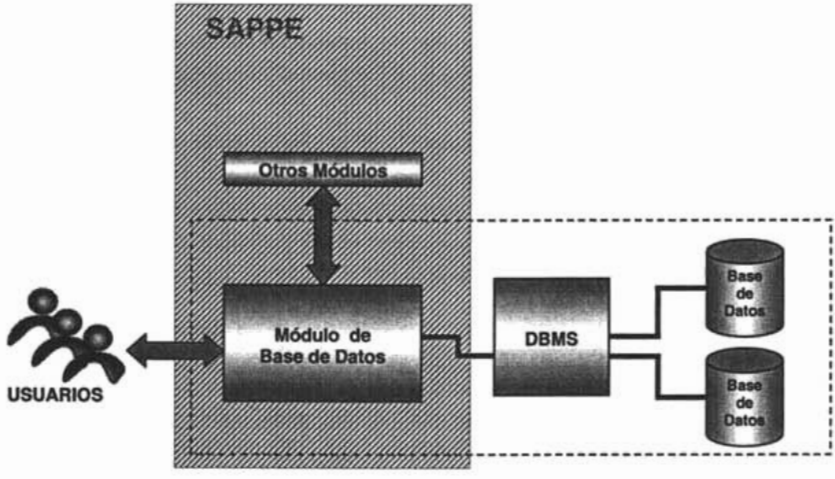


Figura 3.9 Integración del Módulo de BD en SAPPE

Los elementos y estructura del módulo mostrados son el resultado de un cuidadoso análisis de requerimientos que definió las características del diseño. Cada elemento será abordado a detalle en secciones posteriores, por lo pronto únicamente describiremos las funciones generales:

Las Bases de Datos

Son los datos que el sistema necesita, organizados en una estructura definida en función de las necesidades de información tanto de los usuarios como del software. En nuestro caso el diseño considero emplear dos bases de datos para permitir el tratamiento independiente de información según su uso en el sistema.

- Datos para las funciones del software
- Datos para operar el hardware

Sistema Gestor de Base de Datos

Atiende a las llamadas de la aplicación y le proporciona los servicios de consulta y manipulación de datos que requiere. Además de los servicios comunes de un sistema de esta naturaleza como son: Procedimientos almacenados, acceso concurrente a la información y mecanismos de seguridad de integridad de datos.

La aplicación de Base de Datos

Aprovecha las facilidades del SGDB para administrar y manipular la información de Base de Datos con el fin de llevar a cabo las funciones específicas del sistema. Como validar la salida de equipos, mostrar en pantalla el monitoreo de las entradas y salidas del personal al edificio o generar reportes impresos de incidentes, etc.

3.3.1 Los Datos

Las Bases de Datos se incluyeron en la aplicación en respuesta al alto volumen de información que se espera maneje SAPPE. El cual consideramos sería casi imposible manipular dentro del mismo software, además de ineficiente y lento. Por lo que optamos por emplear un medio más apropiado.

El empleo de dos bases de datos nos permitió abarcar todos los datos necesarios para responder a las necesidades de información de todos los involucrados en el sistema. Además que cada base puede crecer y modificarse de manera independiente sin afectar a la otra o a la aplicación. Lo que le da gran flexibilidad y modularidad al software.

Cada base de Datos se originó de un modelo de datos que representa los objetos, personas, hechos y comportamientos que existen en realidad en el sistema. Para ello empleamos el modelo entidad-relación como herramienta de modelación de datos y el modelo relacional para expresar el diseño final.

Así lo primero fue identificar lo que se almacenaría en las bases de datos y definir su estructura y relaciones. Luego, progresivamente trabajamos en modelos más exactos hasta que logramos el grado de detalle donde todos los requerimientos de información fueron contemplados. Finalmente pasamos los modelos elegidos a su forma relacional y verificamos la normalización. A continuación describiremos minuciosamente el diseño de cada una de las bases.

Diseño de la Base de Datos para las funciones del software

Las funciones del software son muchas, de hecho abarcan todo el trabajo del sistema, ya que como hemos mencionado la aplicación es el cerebro que lo controla todo. De ahí que el modelo de esta base datos incluya todos los elementos que integran el sistema a excepción del hardware.

Un modelo de base de datos es una representación del modelo que de la realidad tienen los usuarios y diseñadores del sistema. En nuestro caso la percepción de la realidad a modelar se trata de: "Un Sistema de Seguridad que controla diversos dispositivos de hardware para la protección de equipo y la administración de acceso de personal a las instalaciones de un edificio, así como la identificación y registro de incidentes".

Lo anterior es la descripción más general que podemos dar del sistema, pero aún así es la mejor perspectiva para identificar los detalles más elementales del diseño, como las entidades básicas : usuarios, equipos e incidentes. Y algunas de las relaciones: acceder, salir, registrar, etc.

Antes de ver detalladamente el modelado de la base de datos, la figura 3.2.1.1 es el diagrama entidad-relación donde podemos observar como se integra la información:

- La información de los usuarios incluye datos personales, datos de restricciones de acceso y registro histórico de todas las entradas y salidas efectuadas. El sistema validará el acceso de los usuarios comparando el identificador único de usuario contra los datos contenidos en las tablas hora, día y área de acceso que coincidan con el identificador. Del resultado de la validación dependerá la creación de un nuevo registro en el histórico de las entradas y salidas de usuario o bien la creación de un incidente de usuario por "intento de acceso en hora, área o día no permitido".

- Dado que los administradores del sistema por fuerza deben ser también usuarios con un tipo específico de acceso al sistema y cuentan con datos personales, se incluyeron en el modelo como identidad subtipo, es decir que para que exista un administrador del sistema primero debe existir su registro en base de datos como un usuario del sistema.

- Como parte del proceso de protección de equipo, también en Base de Datos se incluye la información detallada del total de equipos con los que cuenta el edificio. Se considera la información general descriptiva del equipo, información requerida para la validación de salida de equipo con datos de hora y día de salida autorizados así como del responsable por la salida y fecha de devolución. Además de información del estado actual del equipo que permite al sistema tener un seguimiento de hechos tales como: si el equipo esta actualmente en las instalaciones y tiene o no autorización de salida, si el equipo esta afuera o si el equipo fue devuelto. Y por último datos históricos de todos los equipos que han estado fuera. El sistema validará el identificador único del equipo comparando contra los datos autorizados de salida. En caso de resultar positiva la comparación se creará un nuevo registro de salida de equipo, de no ser así se creará un nuevo registro de incidentes de equipo.

- Los incidentes nos permiten llevar un registro histórico de hechos ocurridos sobre las otras entidades del sistema, como intento de acceso de usuario no autorizado o intento de salida de equipo sin autorización. Obviamente este tipo de registros requieren vinculación con los datos de las otras entidades para poder obtener completa información de la situación que se presente. Así los incidentes se asocian con usuarios, equipos, áreas, horas y días.

Aunque el sistema ya integrado es un poco mas complejo que el que se muestra en el diagrama siguiente, cumple su propósito que es mostrar claramente las relaciones existentes entre los elementos de la base.

La composición de elementos se ve con mayor detalle en la estructura de la base de datos mostrada en las figuras 3.11, 3.12, 3.13 y 3.14 donde se observan los campos de información de las tablas, así como el esquema de integridad referencial.

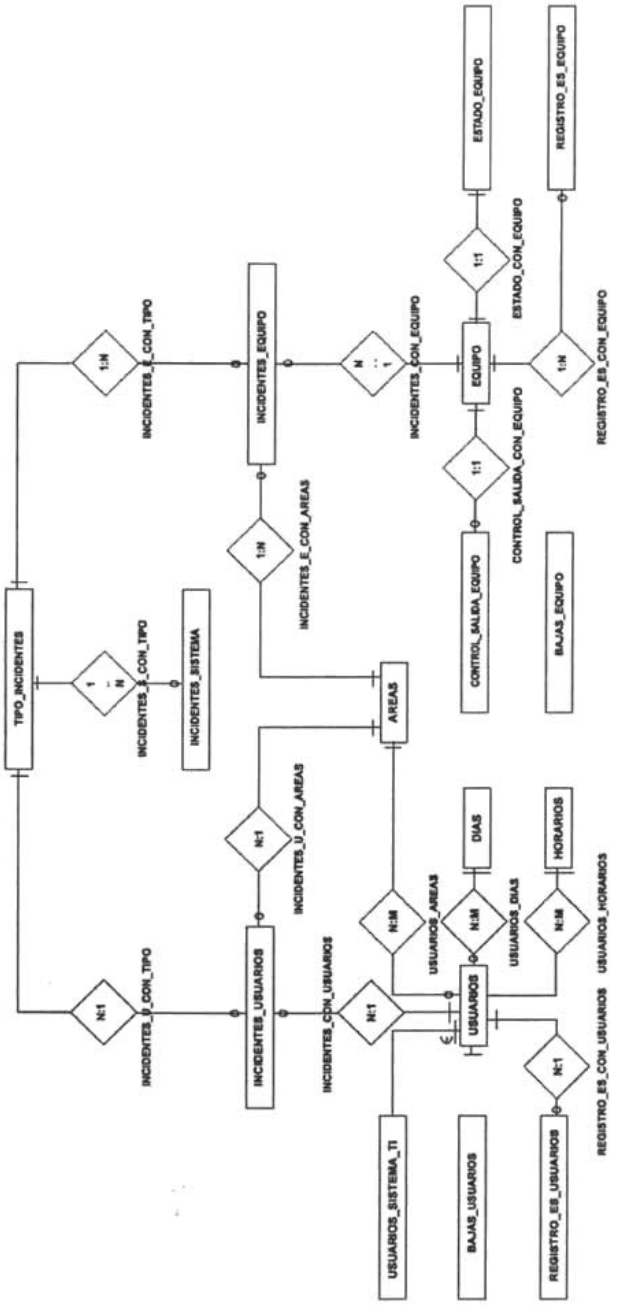


Figura 3.10 Diagrama Entidad-Relación de la Base de Datos

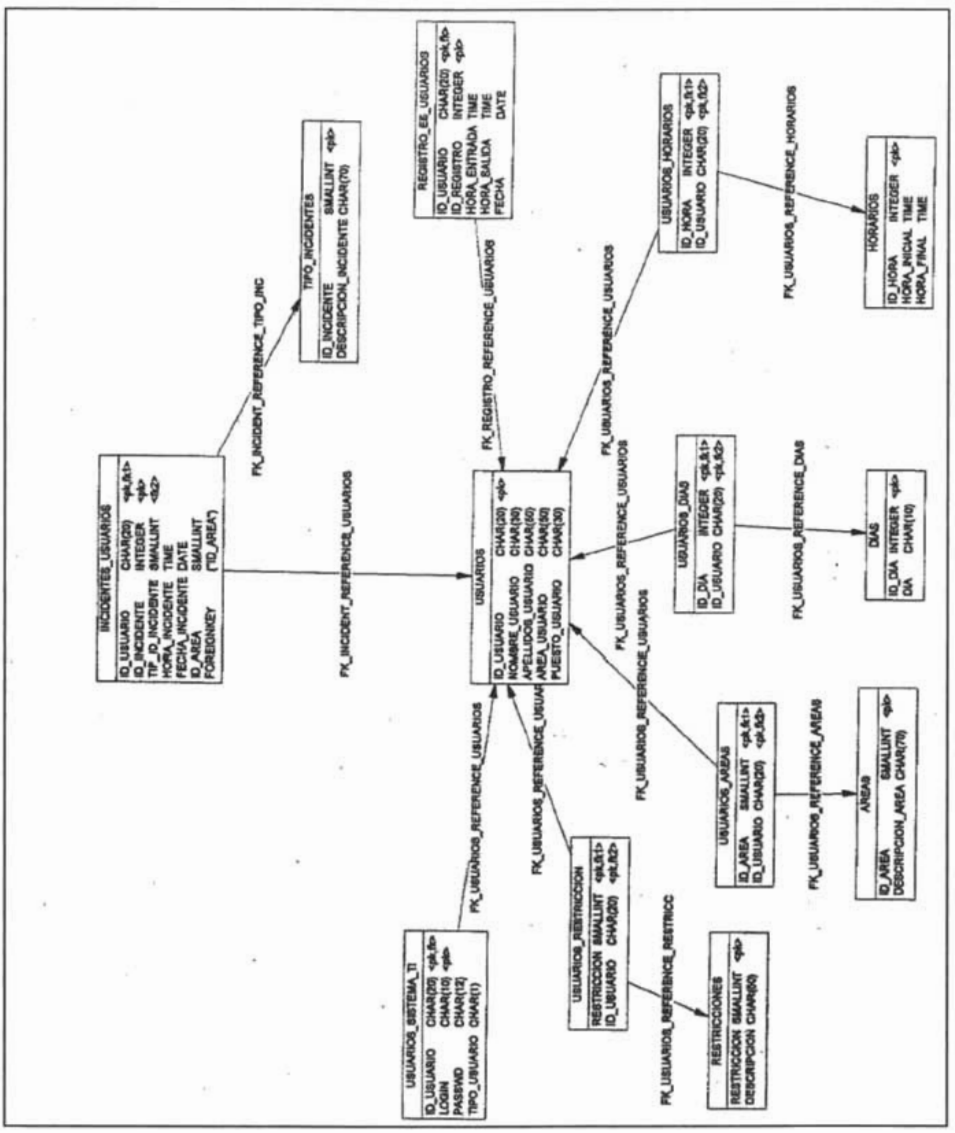


Figura 3.11 Sección usuarios

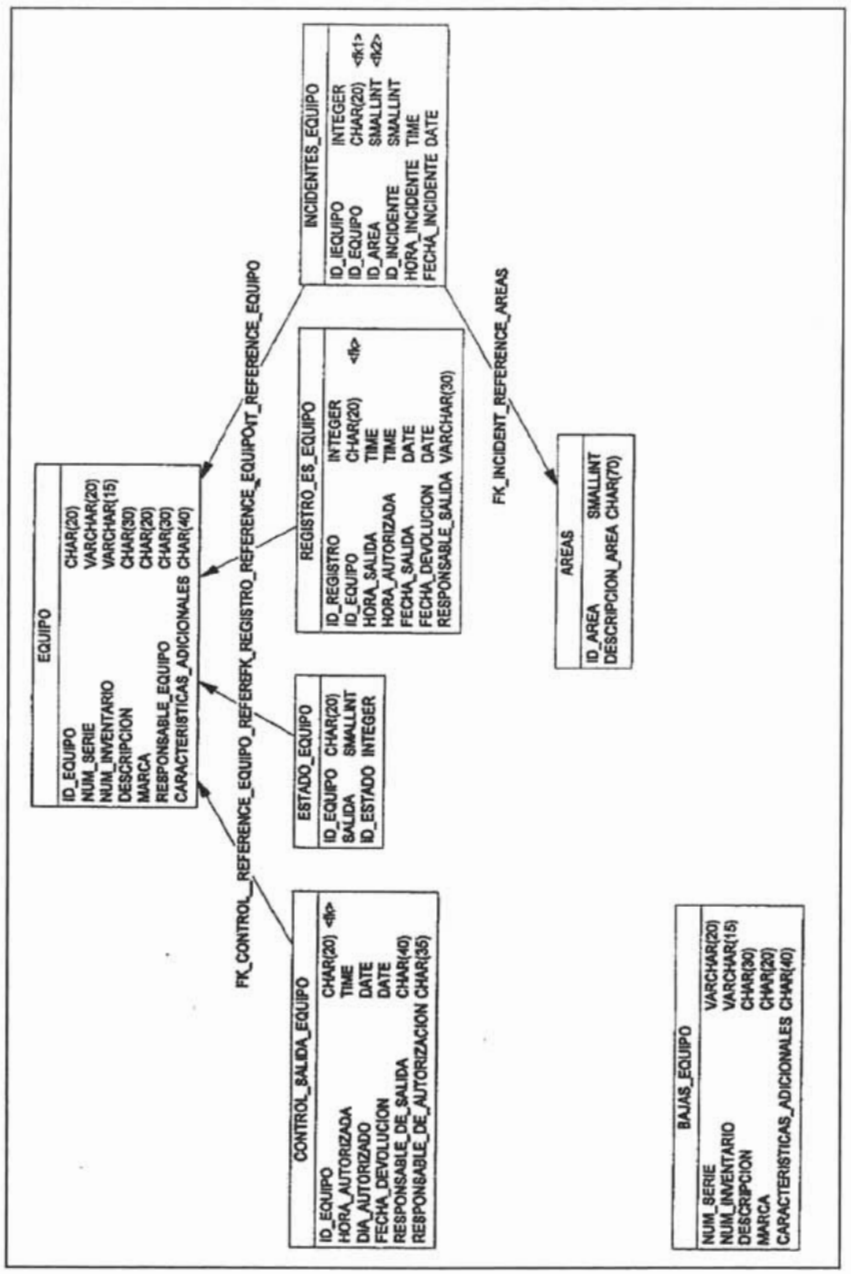


Figura 3.12 Sección Equipo

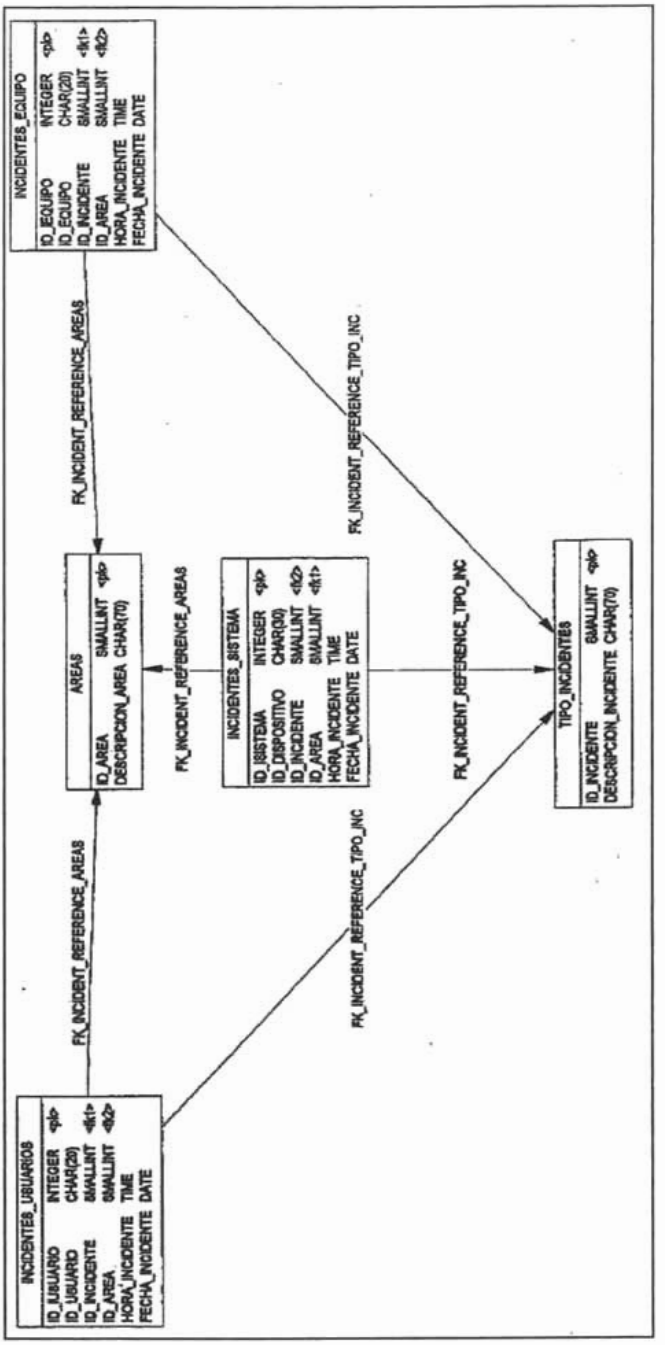


Figura 3.13 Sección Incidentes

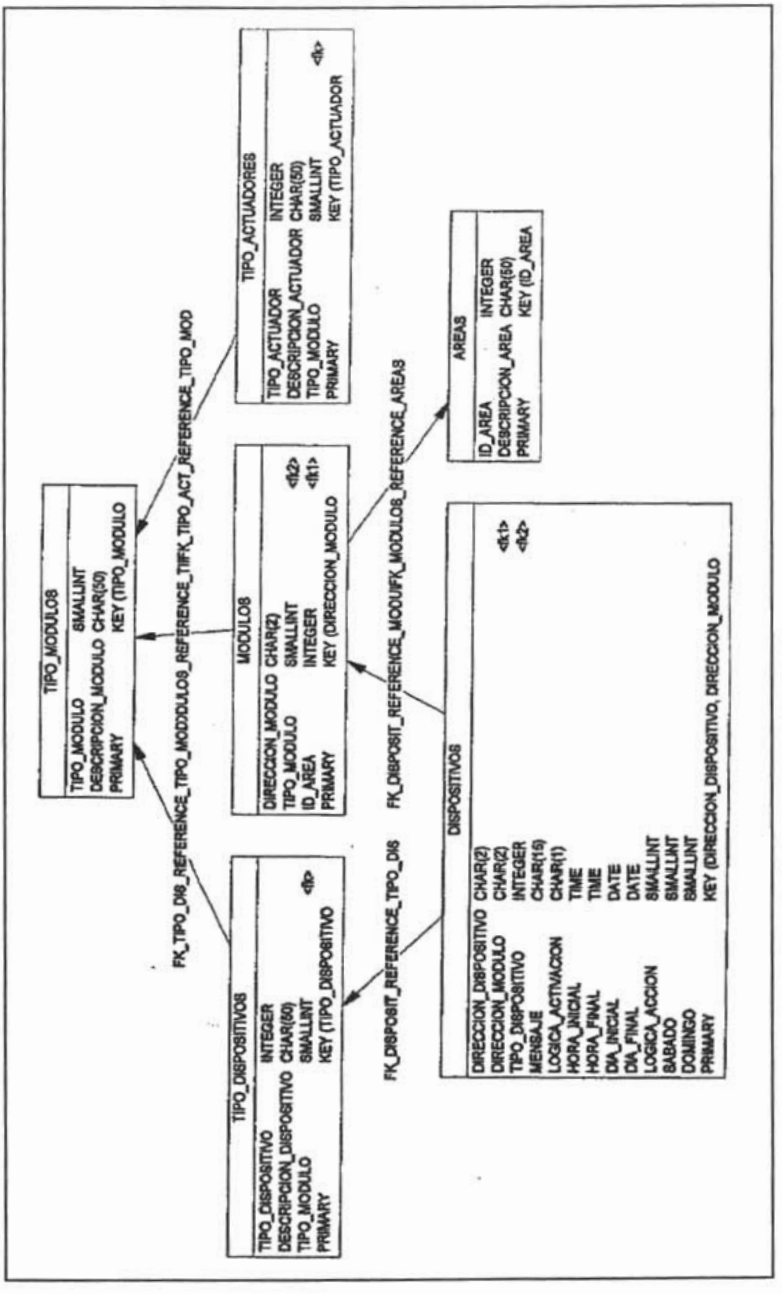


Figura 3.14 Base de Datos de Dispositivos

Un adecuado diseño de base datos garantiza información confiable y disponible en todo momento que se requiera. El modelo mostrado, es el que después de explorar varias alternativas al diseño se apega más al modelo de la realidad operativa y contexto en el que se desempeña la aplicación SAPPE. Responde a las necesidades de información al mismo tiempo que da adecuado seguimiento a los principales elementos que atañen al sistema: usuarios, equipos e incidentes.

Hasta este punto se tiene una una visión integral de todos los elementos que forman parte de la estructura de la base de datos, en las secciones subsecuentes se describirá cada parte en tres bloques: usuarios, equipos e incidentes.

USUARIOS

Una de las líneas principales de seguimiento de información en la Base de Datos son los datos correspondientes a usuarios. La información generada por esta parte de la Base de Datos fundamenta varias de las operaciones del sistema:

- La administración de personal
- Validación de entrada de usuarios
- Despliegue en pantalla de las entradas y salidas
- Registro de incidentes de acceso de usuarios
- Generación de reportes impresos

Para su análisis dividimos los datos en tres secciones:

a) Datos personales
b) Datos de acceso
c) Datos históricos

Datos personales

En esta sección se encuentra la información que define de manera específica al usuario. Se almacenan los datos relativos a sus apellidos, nombre, puesto y lugar donde labora, además que cada usuario es identificado con una llave única en el sistema: la clave almacenada en la tarjeta inteligente que le sirve de acceso. Dicha clave como ya hemos mencionado en la sección de comunicaciones es una cadena irrepetible y en lo sucesivo la denominaremos id_usuario.

La información registrada esta vínculada prácticamente con todas las tablas que forman la sección de usuarios, ya que proporciona la información más importante sobre el resto de los sucesos a los que puede dar seguimiento el sistema: "¿Quién?". Así sabemos cosas como: ¿quién entró o salió del edificio? , ¿Quién trato de entrar sin autorización? ¿Quién autorizo alguna salida de equipo? , ¿Quién extravió su credencial de acceso? , etc.

El vínculo lo efectuamos por medio de el id_usuario que es llave foránea del resto de las tablas, a excepción de la tabla BAJAS_USUARIOS que se trata de un registro histórico de usuarios que no están activos en el sistema y por tanto no cuentan con una credencial con identificador único que les proporcione un id_usuario.

En los casos de las tablas REGISTRO_ES_USUARIOS, INCIDENTES_USUARIOS, USUARIOS_DIAS, USUARIOS_DIAS y USUARIOS_HORAS el incluir el id_usuario como llave foránea fue el resultado de el paso normal de relaciones N:M, 1:N y N:1 al modelo relacional. Pero tuvimos un caso especial, la tabla USUARIOS_SISTEMA_TI que cuenta con la misma llave foránea que las demás, pero es resultado de modelar una entidad subtipo. Para nosotros como diseñadores de la Base de Datos resultaba evidente que quienes van a manejar el software también son usuarios del sistema. Por ello ésta tabla fue creada en el modelo entidad-relación como una entidad subtipo.

Datos de acceso

Los Datos de Acceso, como su nombre lo indica, tienen que ver con las restricciones que los usuarios tendrán para el ingreso al edificio. La sección esta integrada por las tablas: AREAS, DIAS, HORARIOS, USUARIOS_AREAS, USUARIOS_DIAS y USUARIOS_HORARIOS que contienen la información necesaria que el sistema emplea para permitir la entrada a las instalaciones.

Con la finalidad de darle al sistema la mayor flexibilidad, en el diseño consideramos las múltiples opciones de ingreso que una persona pudiera tener:

- Algunos usuarios pueden ingresar a todas las áreas del edificio a toda hora.
- Algunos usuarios pueden ingresar a todas las áreas pero en horas específicas.
- Algunos usuarios sólo tienen acceso a una o varias áreas del edificio a todas horas.
- Algunos usuarios pueden tener acceso a determinada o varias áreas del edificio a toda hora

De acuerdo a lo anterior, las tablas: AREAS, HORARIO y DIAS corresponden cada una con el tipo de restricción que se puede aplicar; por área, por día o por hora. Mientras que las tablas: USUARIOS_AREA, USUARIOS_DIAS y USUARIOS_HORAS son las que indican a quien aplicar que restricción. De esta manera un mismo usuario, por ejemplo: puede tener varios registros en la tabla USUARIOS_AREAS lo que significará que cuenta con el acceso a varias áreas, o bien una sola entrada en dicha tabla que implica que tiene acceso a una única área. Lo mismo será para las demás tablas según los registros que tenga el usuario en la tabla y los datos que contengan tendrá uno o varios días permitidos de acceso, uno o varios horarios. Además un mismo usuario tiene por lo menos un registro en cada una de las tablas para formar el perfil completo del tipo de acceso con el que cuenta.

Lo anterior quedará más claro revisando un poco más a fondo la estructura y relaciones existentes entre las tablas mencionadas:

Las tablas USUARIOS_DIAS, USUARIOS_AREAS y USUARIOS_HORAS propiamente se trata de tablas de intersección que representan la relación N:M existente entre la tablas USUARIOS y AREAS, DIAS, HORARIO. Dichas tablas únicamente tienen los campos provenientes de las llaves primarias de sus tablas padres:

USUARIOS_DIAS (id_usuario, id_area)
USUARIOS_AREAS (id_usuario, id_areas)
USUARIOS_HORAS (id_usuario, id_horas)

Con este tipo de relación, una búsqueda simultánea en las tres tablas por el id_usuario, retornará a la aplicación la información de acceso de ese usuario. Y con la ayuda de las tablas AREAS, DIAS, HORARIO y USUARIOS podemos obtener las descripciones de área, horarios y datos del usuario. Cabe mencionar que para agilizar la validación que al momento de leer una credencial en la aplicación consideramos hacer la búsqueda por el id_usuario en base de datos y únicamente esperamos valores enteros de retorno que sirven como banderas para activar la acción propia, como abrir la puerta. Las descripciones se incluyeron en el diseño para satisfacer el detalle de información requerido por las personas que manejarán el sistema, como el mostrar en pantalla los accesos y salidas de personal al edificio incluyendo el área o el reporte impreso de incidentes, etc.

Datos históricos

La sección de Datos Históricos integra la información con respecto a usuarios, que no es de utilidad para la operatividad básica del sistema, sino de interés administrativo, se compone por las tablas: REGISTRO_ES_USUARIOS y BAJAS_USUARIO.

La tabla REGISTRO_ES_USUARIOS contiene información sobre el acceso y salida de usuarios al edificio. La forman los campos id_registro, id_usuario, hora_entrada, hora_salida, area y fecha que en conjunto describen el hecho de la entrada o salida de un usuario a las instalaciones. La información que se registrará planeamos que sea del tipo histórico, es decir que abarque tanto los acceso y salidas del día en curso como de fechas anteriores. Siendo la aplicación quien se encargue de dar formato y presentar al usuario únicamente la parte de su interés. Los campos id_usuario y área, son llaves foráneas que nos permitirán saber exactamente quien entra y en que área.

Por otra parte la tabla BAJAS_DE_USUARIOS almacena la información de las personas que ya no cuentan con acceso al edificio, por distintas razones: porque ya no laboran en las instalaciones, ya terminó su período de tesis o servicio social

, etc. Los campos de la tabla son : nombre_usuario, apellidos_usuario, area_usuario y puesto_usuario.

EQUIPOS

Esta sección es homóloga a la sección de usuarios. De hecho los datos que la integran sustentan el mismo tipo de funciones del sistema con la diferencia que en esta ocasión se refieren a equipos:

- La administración de equipos
- Validación de salida de equipo.
- Monitoreo de salida de equipo.
- Seguimiento del estado de los equipos
- Generación de reportes

Con el fin de mantener un diseño homogéneo y fácil de entender, los datos se dividieron igual que los de usuarios, según sus características y finalidad en el sistema:

a) Datos de los equipos
b) Datos de autorización de salida
c) Datos históricos

Datos de los equipos

La información contenida en esta sección es de carácter descriptivo, incluye las características que definen por completo un equipo, como son: el número de serie, el número de inventario, el tipo de equipo del que se trata, la marca, la descripción y el responsable del equipo. Además de un identificador único que es el que se detecta y válida en la Base de Datos al momento de salir un equipo.

El identificador único es un cadena irrepetible grabada en el transmisor-receptor que se coloca en cada uno de los equipos que se desea proteja el Sistema. Dentro de la base de datos este dato es el campo ID_EQUIPO. El resto de las características mencionadas también corresponden cada una a campos de la tabla EQUIPO y son: NUM_SERIE, NUM_INVENTARIO, DESCRIPCION, MARCA, CARACTERISTICAS_ADICIONALES Y RESPONSABLE_EQUIPO.

Todos los campos son importantes para poder definir claramente a que equipo afectan determinadas situaciones, por ejemplo , saber exactamente que equipo salió con autorización o cual sufrió un intento de robo, etc. Pero el ID_EQUIPO es el más significativo porque es precisamente quien relaciona al equipo con la situación que le atañe. ID_EQUIPO es la llave primaria de la tabla EQUIPO y tiene relación con el resto de las tablas que forman el bloque de información sobre

equipos a excepción de la tabla BAJAS_EQUIPO. Así una consulta lanzada a la Base de Datos buscando por las coincidencias del ID_EQUIPO en todas las tablas, nos daría un panorama a detalle de todo lo que concierne a un equipo: su descripción, su estado, si salio o no, etc.

El vínculo mencionado se estableció migrando a ID_EQUIPO como llave foránea para el resto de las tablas. Así se expresaron en forma relacional la relaciones 1:1 y 1:N manifestadas en el modelo entidad-relación de la sección equipos.

Datos de autorización de salida

Permitir o no la salida de un equipo es crucial para la protección de equipo. De ahí que la información contenida en esta sección sea de suma importancia, ya que permite la validación de cada equipo que se detecta a la salida de las instalaciones.

En contraste con el acceso de usuarios donde buscamos dar el mayor número de opciones posibles para flexibilizar la entrada a las instalaciones. En la salida de equipos limitamos las condiciones de salida al máximo con el fin de disminuir las posibilidades de un robo. Así un equipo puede salir sólo si:

- Alguna persona responsable por los bienes que se encuentran en el edificio lo autoriza.
- Cumple exactamente con la hora y fecha específicos de salida.

Dichas condiciones se expresan en la tabla CONTROL_SALIDA_EQUIPO en los campos HORA_AUTORIZADA, DIA_AUTORIZADO, FECHA_DEVOLUCION, RESPONSABLE_DE_SALIDA y RESPONSABLE_DE_AUTORIZACION. Esta tabla contendrá unicamente los registros de los equipos con autorización de salida y es precisamente contra la que se comparará el identificador de equipo leído al momento de pasar un equipo en las puertas

Datos históricos

Al igual que los datos históricos de usuarios, en esta parte se guardan datos que permitirán consultar información de interés meramente administrativo. Se compone por las tablas BAJAS_EQUIPO y REGISTRO_ES_EQUIPO.

En BAJAS_EQUIPO se encuentran los quipos que a juicio de los responsables por los bienes de las instalaciones ya no es necesario proteger y por tanto ya no cuentan con un transmisor-receptor. También se hizo esta tabla pensando en apoyar el control de equipos dados de baja del inventario UNAM. En base a ella se podrán generar reportes de equipo que ya no es funcional.

El REGISTRO_ES_EQUIPO es un histórico de todos los equipos que alguna vez han salido de las instalaciones. Una consulta en la tabla por el identificador de equipo nos permitirá conocer exactamente cuantas veces ha salido ese equipo, la fecha de salida en cada ocasión y el responsable de salida.

INCIDENTES

Los incidentes son eventos negativos que ocurren en el entorno del Sistema. Dichos eventos ponen en riesgo a los elementos del Sistema o afectan su funcionalidad, por eso se registran en Base de Datos. El objetivo es saber lo que pasa y así poder ejercer algún tipo de control sobre ellos, ejecutando alguna acción por parte del sistema o con la intervención humana.

Debido a que los incidentes afectan directamente a alguno de los elementos básicos de la función del sistema, se dividieron en tres: incidentes de usuario, incidentes de equipo e incidentes de sistema. Cada tipo corresponde a una tabla en la Base de Datos con el mismo nombre: INCIDENTES_USUARIOS, INCIDENTES_EQUIPO e INCIDENTES_SISTEMA.

En cada una de las tablas se define por completo el incidente ocurrido: la hora, el día, la descripción y exactamente donde ocurrió y a quien o que afectó. Así la estructura de las tres tablas es la misma en los campos: ID_INCIDENTE, HORA_INCIDENTE, FECHA_INCIDENTE, TIPO_INCIDENTE y AREA. A excepción de ID_EQUIPO, ID_DISPOSITIVO e ID_USUARIO que son campos que corresponden cada uno a una tabla específica según el incidente que se trate.

Estos tres últimos campos completan a detalle la descripción del incidente ya que a través de ellos es posible conocer características específicas sobre quien o que afectaron los hechos. Esto es, ID_EQUIPO e ID_USUARIO son llaves foráneas provenientes de las tablas EQUIPO y USUARIOS que con una consulta compuesta nos permitirán conocer el nombre, apellidos, puesto ,el tipo de equipo, marca, etc. de usuario o equipo afectados Por otra parte ID_DISPOSITIVO es un dato que obtiene y formatea la misma aplicación de descomponer la cadena de recepción que notifica el incidente.

3.3.2 Diseño del módulo de base de datos

Propiamente el módulo de base de datos es la interfaz e implementación que provee la conexión, inserción, extracción y proceso de datos para compartirlos o presentarlos en el formato adecuado a los usuarios y otros módulos del software. Se divide en las siguientes partes:

- Funciones auxiliares
- Procesamiento de Información para la operación de SAPPE
- Conexión a Base de Datos
- Transacciones a la Base de Datos
- Reportes

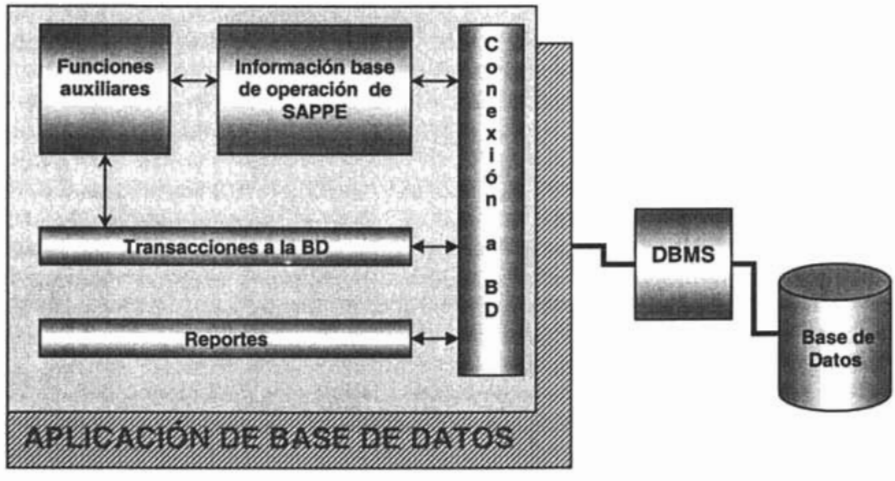


Figura 3.15 Bloques del módulo de Base de Datos

3.4 Interfaz de Usuario

La carta de presentación de cualquier aplicación es sin duda su interfaz de usuario. Diseñar consistentemente la interfaz facilita al usuario la correcta operación del sistema y el aprovechamiento total del potencial del software. Por ello su diseño no debe limitarse únicamente a las características más tangibles como la apariencia estética o comportamiento, debe además enfocarse directamente al uso para el cual la aplicación está destinada.

SAPPE es una aplicación para la administración y control de un sistema de seguridad, por lo tanto gran parte de sus procesos actúan de manera autónoma, sin embargo existen operaciones que dependen de la interacción del usuario con el sistema lo que conlleva a generar una serie de pantallas que faciliten estas tareas.

Los principales intereses al elaborar el diseño visual del programa fue crear una interfaz cuya manejo fuera intuitivo y fácil de aprender para el usuario. Así como una presentación transparente y organizada de la información. Se consideraron distintos escenarios para administrar por una parte la base de datos y por otra parte el hardware, así como una pantalla principal que unificara ambos procesos, tal como podemos ver en el siguiente diagrama.

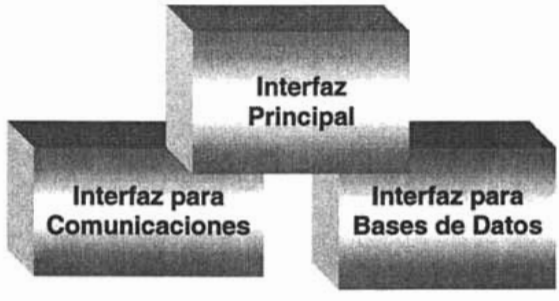


Figura 3.16 Interfaces Básicas

A partir de este diagrama describiremos la estructura de cada una de las interfaces que conforman la presentación gráfica de SAPPE.

3.4.1 Interfaz Principal

La interfaz principal tiene como objetivo introducir al usuario dentro del entorno de SAPPE, involucrándolo de una manera sencilla con los principales procesos del sistema.
Para ello consideramos los siguientes elementos:

- Un seguimiento y monitoreo de operaciones que muestre al usuario en cada momento las actividades que realiza el sistema.
- Un menú que permita el acceso a las funciones del sistema tal como son las administración y control de las comunicaciones y la administración de la base de datos.
- Un acceso controlado al sistema mediante restricciones de seguridad a nivel de usuario que nos aseguren que los diferentes tipos de usuarios puedan acceder a ciertas partes del sistema con privilegios determinados.

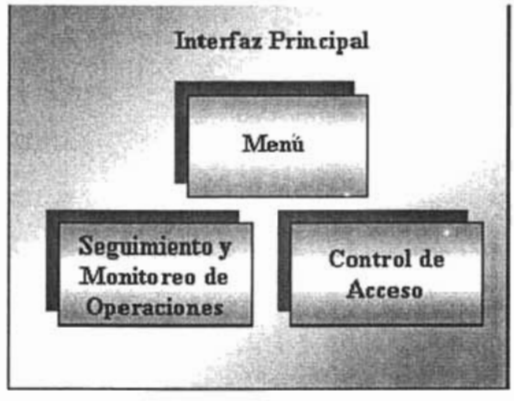


Figura 3.17 Elementos que constituyen la interfaz principal

Una parte elemental es sin duda la disposición de todos los objetos dentro de la interfaz principal. Ya que es importante colocarlos estratégicamente de manera que el usuario pueda identificar cada uno de ellos de forma clara así como proporcionar un aspecto visual agradable que estimule el interés del usuario.

La interfaz principal comprendió dos etapas de diseño. La primer etapa estuvo orientada al aspecto funcional del programa mientras la segunda etapa se enfocó al aspecto estético y ergonómico de las interfaces

Interfaz Principal (Primer Etapa)

Durante esta primer etapa concentramos nuestra atención en la información que deseábamos transmitir al usuario. Por lo tanto incluimos todos los elementos necesarios para ambientar al usuario en todos los servicios de los que podría gozar al utilizar el sistema, tales como:

- Notificación de fallas en los dispositivos de comunicación.
- Notificación de intento de salida de equipo no autorizada.
- Monitoreo de los accesos y salidas del personal.
- Acceso al sistema.

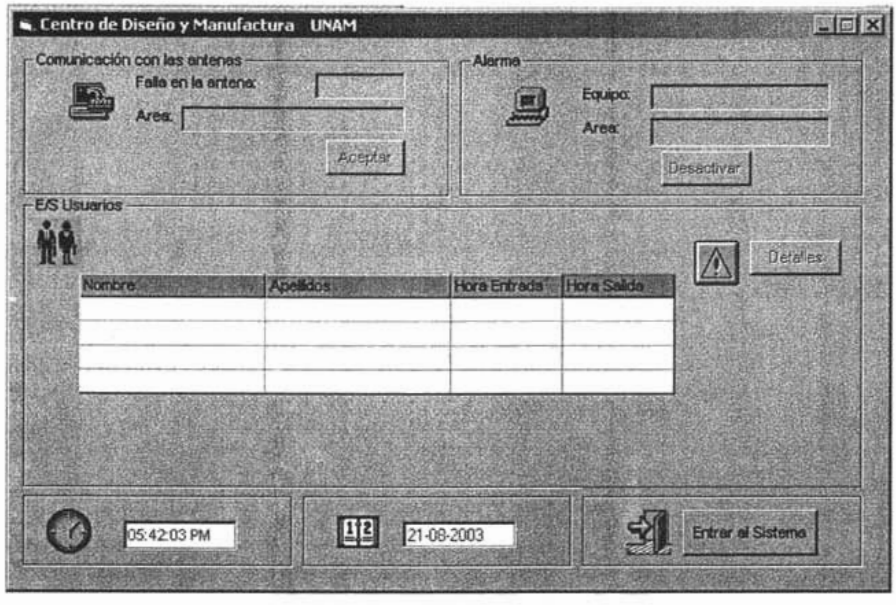


Figura 3.18 Pantalla de Interfaz Principal (Primera Etapa)

Hicimos uso de recursos multimedia muy sencillos y cambio de colores para resaltar cuando se estuviera dando un evento de magnitud trascendente como es el robo de equipo o la manifestación de fallas en el funcionamiento del hardware.

Mediante colores vistosos destacamos el área de la pantalla dedicada al monitoreo de una acción determinada o bien desplegamos señales de alerta y animaciones que hicieran más claro cada operación logrando de esta manera atraer especial atención en él.

En el caso de fallas de sistema nuestro principal interés fue informar a nuestros clientes de la falla de algún dispositivo especificando su ubicación para facilitar la tarea de reparación y mantenimiento del mismo.

Uno de los principales propósitos del sistema es la protección del equipo por lo que decidimos poner mayor énfasis en la representación gráfica de este evento. Visualmente predominamos la zona de monitoreo de equipo no sólo por la distinción de color sino haciendo uso de una animación gráfica en sincronía con una alarma sonora que permitiera destacar un estado de alerta, asimismo haciendo uso de cuadros de texto identificamos el tipo de equipo que estaba siendo sustraído de las instalaciones.

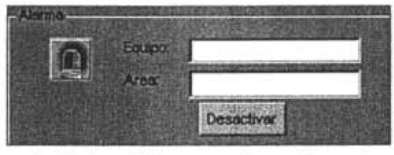


Figura 3.19 Pantalla para desactivar alarma

El monitoreo de acceso y salida del personal fue representado por el manejo de celdas donde se puede apreciar la identificación del personal así como la hora en que está entrando o saliendo de las instalaciones. Aunado a esta información hicimos uso de íconos para representar anomalías tales como intento de accesos no autorizados, que permitían al usuario administrador tener completo control sobre los incidentes ocurridos durante el día.

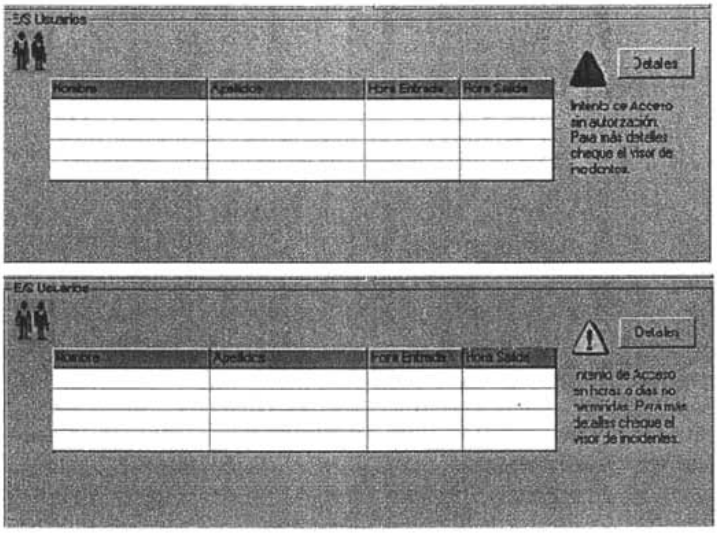


Figura 3.20 Pantalla con iconos que comunican anomalías en el sistema

Interfaz Principal (Segunda etapa)

Desde un criterio funcional la interfaz principal estaba cumpliendo sus objetivos, sin embargo, existían ciertos detalles que requerían especial atención:

- El primero, sin duda, era que la interfaz principal se tenía muchos elementos que podían confundir en algún momento al usuario.

- Visualmente la interfaz carecía de uniformidad en cuanto a textura, colores e imágenes que ofrecían al usuario un programa poco atractivo.

- Por otra parte teniendo conciencia de que existían dos tipos de usuarios que harían uso de este software determinamos que la información de ambos no podía ser desplegada en la misma pantalla ya que podría distraer la atención del usuario hacia operaciones no concernientes con su capacidad de usar el sistema.

- Finalmente consideramos que la notificación de eventos debía desplegarse independiente de la pantalla principal de manera que su manifestación asegurara la atención del usuario.

Durante esta etapa nos dedicamos a valorar el aspecto estético de la interfaz reorganizando los elementos y homogeneizando visualmente sus componentes. Hicimos uso de nuevos objetos que enriquecieran el aspecto físico de la pantalla y facilitaran al usuario su interacción con el sistema.

El segundo diseño se apegó muchos más a los elementos considerados para la interfaz principal: Un menú, seguimiento y monitoreo de operaciones, acceso al sistema. Lo que dio como resultado un diseño mucho más claro y agradable para el usuario.

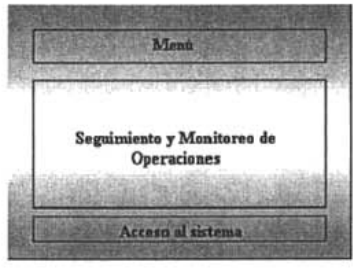


Figura 3.21 A) Elementos de Interfaz Principal

Figura 3.22 B) Elementos de Interfaz Principal

Menú

Un menú sencillo permite al usuario presentar de una forma clara y precisa las opciones a las que tiene acceso. Partiendo de esta premisa y considerando que nuestro sistema está conformado por dos módulos principales: comunicaciones y Bases de Datos decidimos estructurar nuestro menú con dos opciones para ingresar a cada uno de estos módulos (representados por interfases) así como una opción adicional de ayuda que oriente al usuario sobre el uso del sistema.

Asimismo consideramos la utilización de íconos en el menú que permitieran al usuario familiarizarse simbólicamente con cada una de las opciones. El manejo de íconos además de ser una explicación gráfica de las distintas operaciones del sistema ofrecería al usuario un programa visiblemente agradable y amigable.

Un paso importante anterior al diseño y selección de colores de los íconos fue el definir el color de fondo de la interfaz, para el cuál optamos por un color que resultara agradable y suave a la vista de nuestros clientes. Como en cualquier producto de software la selección de colores y texturas es sumamente importante ya que un programa debe ser funcional pero además debe tener una presentación atractiva que acapare la atención del usuario.

Figura 3.23 Menú Gráfico

Monitoreo y notificaciones de alerta

Para determinar el seguimiento y monitoreo de operaciones del sistema consideramos las principales bondades que ofrecería el sistema al usuario. Inicialmente partimos de las características que debe ofrecer un sistema de seguridad y la importancia de mantener al usuario informado sobre los eventos ocurridos durante su operación, para derivar finalmente en los detalles fundamentales a los cuales se debe poner singular atención:

- Monitoreo de las entradas y salidas del personal.
- Monitoreo de la salida de equipo.
- Notificaciones de alerta sobre eventos especiales.

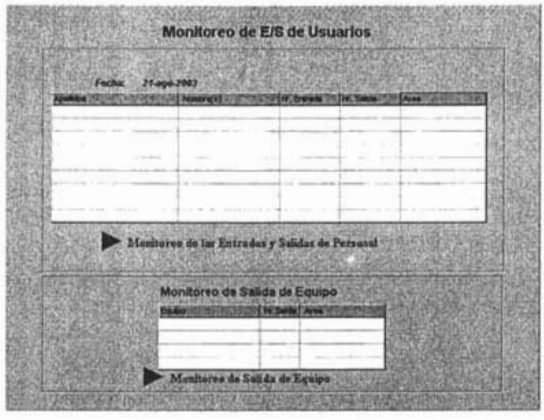


Figura 3.24 Pantalla monitoreo

Cada elemento informativo debe presentar en forma clara un reporte substancial y resumido del aspecto al que hace alusión. El monitoreo del personal debe presentar un registro continuo del acceso y salida de cada individuo así como el horario y el área de su ubicación actual. El monitoreo de equipo, por otra parte, va a permitir al usuario del sistema saber en que momento está saliendo un equipo con permiso de las instalaciones, y tener control sobre el traslado de dicho equipo sobre distintas áreas del edificio controlado.

Sin duda las notificaciones de alerta sobre eventos especiales suponen una atención particular, ya que al ser SAPPE un programa dedicado a un sistema de seguridad, tiene como principal objetivo prevenir y alertar sobre situaciones de riesgo como son el robo de equipo, accesos no autorizados y fallas importantes del sistema. Para ello generamos pantallas independientes que puedan notificar datos relevantes sobre un incidente de esta naturaleza como son hora, ubicación y descripción del suceso. Estas pantallas fueron diseñadas con el objetivo de atraer

la completa atención del usuario por lo que seleccionamos colores llamativos apoyados por imágenes que a simple vista dieran un enfoque claro de la situación que se está presentando.

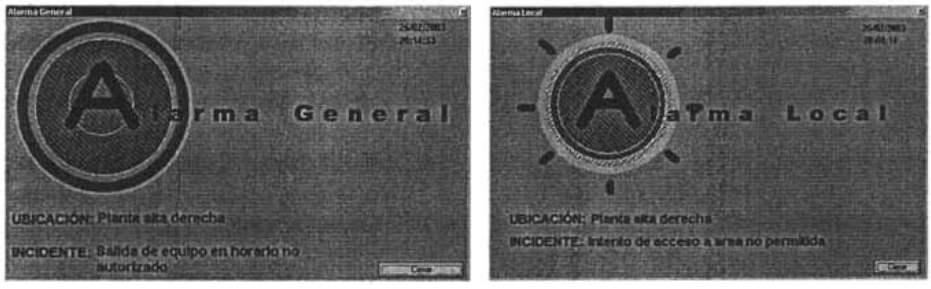


Figura 3.25 Pantallas de notificación de alarma

Acceso al sistema

Como habíamos mencionado anteriormente esta etapa será el control de acceso al sistema, determinando las capacidades de aplicación del usuario sobre el sistema de acuerdo con los privilegios otorgados por un administrador. De acuerdo a la información proporcionada durante ese proceso se revelará una capa distinta de la interfaz subsiguiente que limite o confiera propiedades para manipular la información y control del programa.

Para ello decidimos agregar un cuadro de diálogo que se despliegue al pulsar cualquier opción del menú cuestionando sobre la identidad del usuario que desea ingresar al sistema y comprobando la veracidad de los datos ingresados por la persona; siendo de esta manera un filtro entre la interfaz principal y las pantallas siguientes.

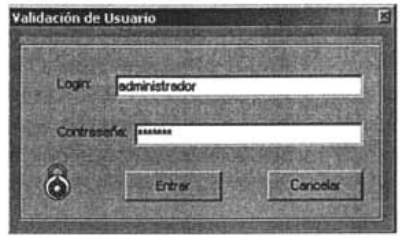


Figura 3.26 Cuadro de diálogo de acceso al sistema

3.4.2 Interfaz para Base de Datos

El objetivo principal de la interfaz diseñada para la base de datos es facilitar todas las actividades comunes como son introducir, modificar y consultar información, así como la generación de reportes.

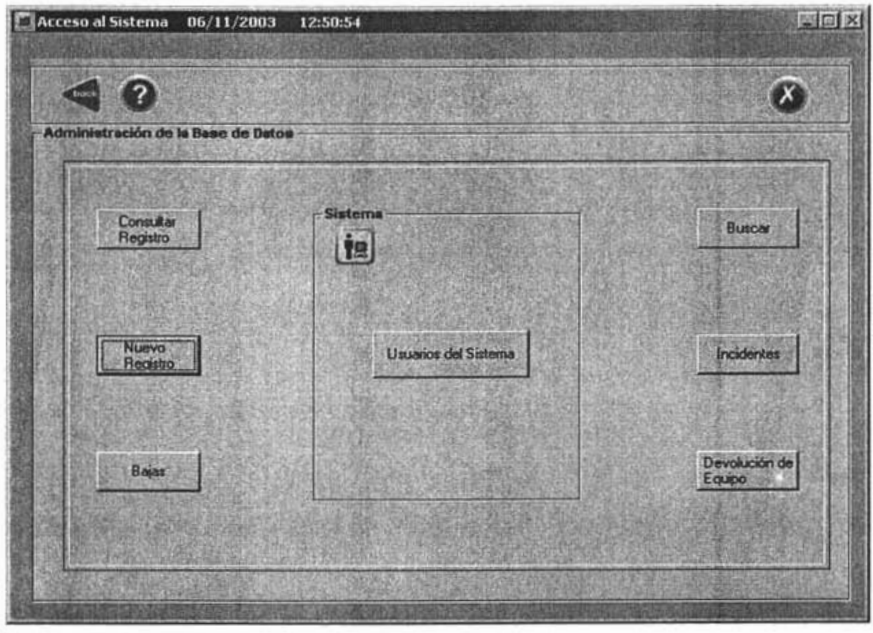


Figura 3.27 Interfaz de Base de Datos

La parte más extensa en despliegue de pantallas se concentró en la administración de la Base de Datos debido a que cada acción implica un conjunto de opciones específicas que, por motivos de claridad, decidimos presentarlas separadamente.

Como mencionamos anteriormente la administración de la Base de Datos implica consultas, modificaciones, altas y bajas, búsqueda de información, etc. Por lo tanto y con el objetivo de no saturar al usuario con todos los procesos implicados en este módulo, presentamos cada operación con una clasificación clara. Para ello determinamos las transacciones principales:

- Consulta de registros.
- Alta de registros.
- Baja de registros.

- Búsqueda de información.
- Reportes de Incidentes.
- Devolución de Equipo.
- Administración de usuarios del sistema.

Una parte indispensable para una correcta operación del sistema es la claridad con que presentamos las opciones y la facilidad que tienen el usuario para aprender a manipularlas, por lo que decidimos presentar una interfaz inicial que conlleve posteriormente a la ampliación de cada opción seleccionada.

Los componentes físicos utilizados para esta interfaz fueron botones y menú con íconos los cuales se situaron de forma estratégica y ordenada dentro de la pantalla.

La intención del menú de íconos fue presentar las opciones más generales como son: regresar a la pantalla anterior, ayuda y salida del sistema; de manera que el usuario pudiera identificarlas inmediatamente al ubicarlas en la parte superior de la interfaz y resaltándolas con íconos que en color, textura y forma están armonizados con el menú dispuesto en la interfaz principal.

Figura 3.28 Menú de iconos

Para poder llevar a cabo cada una de las transacciones principales con la Base de Datos dispusimos de botones cuya acción despliega una pantalla con opciones más particulares acerca de la selección realizada.

A continuación desglosaremos de manera sencilla cada una de las opciones de la interfaz principal de la base de datos explicando sus principales características.

Consulta de registros

La función esencial de esta opción es permitir al usuario realizar búsquedas en la base de datos.

Para facilitar la exploración de datos dispusimos de elementos configurables que permitieran al usuario realizar búsquedas específicas de acuerdo a sus intereses particulares. De esta manera propusimos una interfaz que ofrece al usuario un amplio rango de combinaciones de búsqueda que parte de la información más general hasta datos más específicos. La información proyectada como resultado de una consulta se muestra en tablas organizadas de manera clara y precisa.

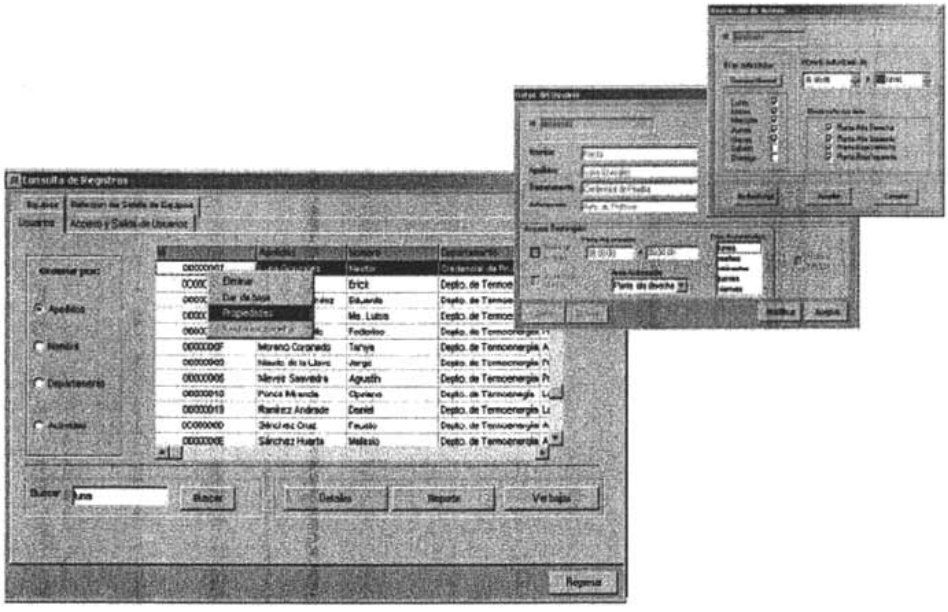


Figura 3.29 Consultas de Registros

Para facilitar la exploración de datos dispusimos de elementos configurables que permitieran al usuario realizar búsquedas específicas de acuerdo a sus intereses particulares. De esta manera propusimos una interfaz que ofrece al usuario un amplio rango de combinaciones de búsqueda que parte de la información más general hasta datos más específicos. La información proyectada como resultado de una consulta se muestra en tablas organizadas de manera clara y precisa.

Un propósito adicional de presentar la información en tablas es protegerla de incidentes que puedan ocasionar alteraciones no controladas en los registros o pérdida de datos. Por lo tanto esta interfaz ofrece opciones adicionales para poder operar sobre un registro particular, de manera que se puedan obtener datos más específicos o bien modificar la información, siempre que el usuario cuente con los privilegios para realizar dicha acción.

A través de esta interfaz el usuario podrá operar directamente sobre los registros teniendo la capacidad de eliminar, modificar y dar de baja registros mediante opciones desplegadas en un menú flotante.

Alta de registros (Nuevo registro)

Este formulario va a permitir al usuario crear y almacenar un nuevo registro en la base de datos.

La interfaz permite al administrador almacenar información concerniente a un usuario o equipo, orientándolo en el llenado de los campos de manera clara y precisa. Finalizando la acción mediante el simple clic de un botón.

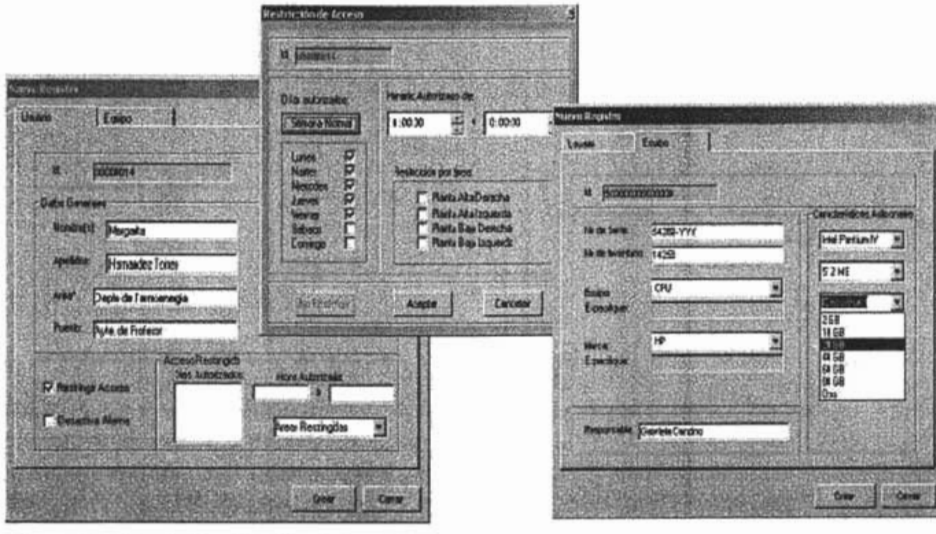


Figura 3.30 Pantallas de Alta de Registros

Baja de Registros (Bajas)

Mediante esta interfaz el usuario podrá dar de baja un registro de la base de datos.

Opciones como eliminar, modificar y dar de baja registros requieren cuestionar previamente al usuario sobre la realización o cancelación de dicha acción; previniendo, de esta manera, errores que puedan llevar a la pérdida de información. En el caso particular de esta pantalla se requiere autentificar la información del usuario o equipo insertando la clave principal del registro, al que procederá un formulario con los datos completos. Una vez concluida la acción la información correspondiente será desplazada a una tabla para mantener la información en caso de consulta posterior pero sin ningún atributo operativo.

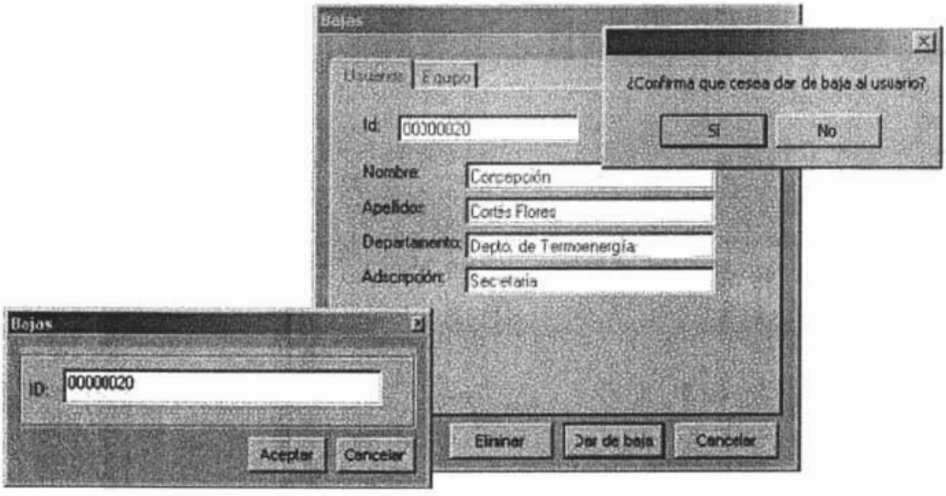


Figura 3.31 Pantallas de Baja de Registros

Opciones como eliminar, modificar y dar de baja registros requieren cuestionar previamente al usuario sobre la realización o cancelación de dicha acción; previniendo, de esta manera, errores que puedan llevar a la pérdida de información. En el caso particular de esta pantalla se requiere autentificar la información del usuario o equipo insertando la clave principal del registro, al que procederá un formulario con los datos completos. Una vez concluida la acción la información correspondiente será desplazada a una tabla para mantener la información en caso de consulta posterior pero sin ningún atributo operativo.

Búsqueda de información (Buscar)

Esta interfaz es muy similar, en operación, al formulario de consulta de registros. Sin embargo, su propósito está orientado a la búsqueda general de datos correspondientes a un criterio propuesto por el usuario.

La pantalla es muy sencilla y fácil de operar. El usuario puede elegir entre búsqueda de usuarios o equipos, para posteriormente insertar los detalles particulares de dicha búsqueda en el único campo presentado en la pantalla. La exploración se realiza en todas las tablas y los resultados son presentados ordenadamente en una tabla.

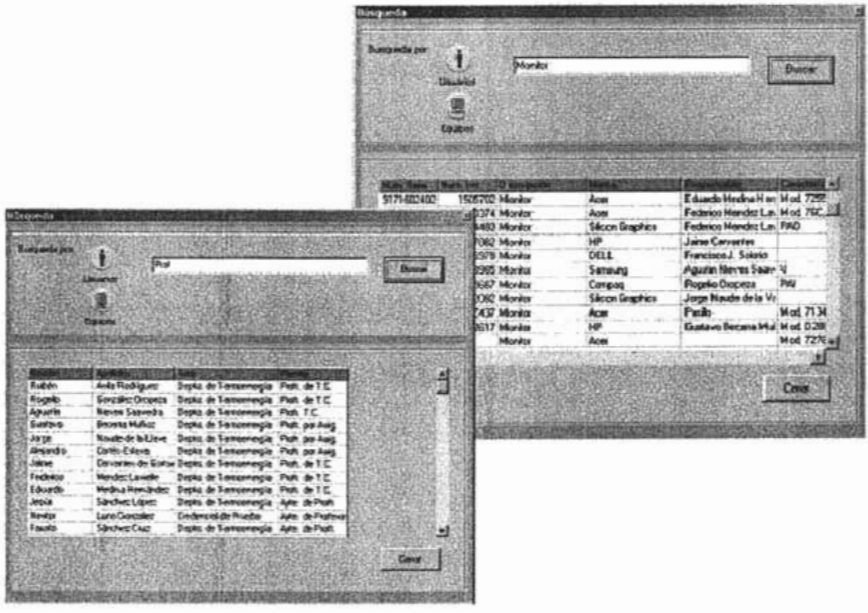


Figura 3.32 Pantallas de búsqueda de información

Reporte de Incidentes (Incidentes)

Este formulario despliega de manera clasificada los incidentes ocurridos de acuerdo a tres criterios: Incidentes relacionados con los usuarios, incidentes relacionados con equipos e incidentes relacionados con el sistema físico. Dicha información se expone en una tabla describiendo de manera general el suceso, la hora y fecha del incidente.

Para facilitar al usuario la búsqueda específica de información dispusimos de elementos que admiten la selección de fechas y horas, filtrando los datos a partir de estos criterios. Asimismo mediante un menú flotante el usuario puede acceder a detalles particulares del incidente seleccionado, los cuales son expuestos en otra pantalla.

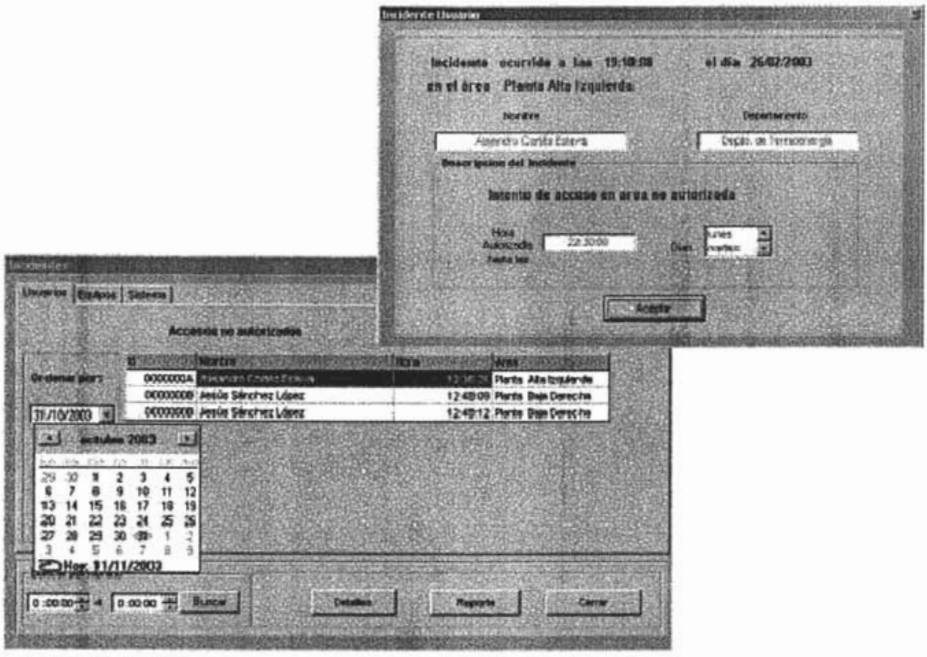


Figura 3.33 Pantallas de Reporte de Incidentes

Devolución de equipo

Esta pantalla tiene como un único proceso registrar cuando un equipo es devuelto a las instalaciones. Por lo que su interfaz es muy simple; presentando la información concerniente a la salida del equipo así como un botón completamente identificado a través del cual se realizará el evento. Una vez que se ha ejecutado dicha acción el equipo queda protegido nuevamente por el sistema de seguridad.

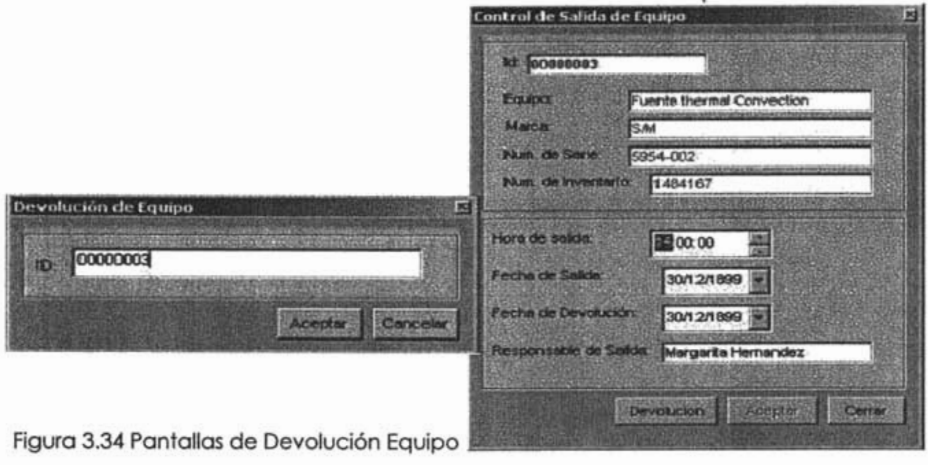


Figura 3.34 Pantallas de Devolución Equipo

Usuarios del sistema

En la parte central de la interfaz principal ubicamos una opción de suma importancia: los "usuarios del sistema", que nos va a permitir consentir facultades particulares de acceso al sistema.

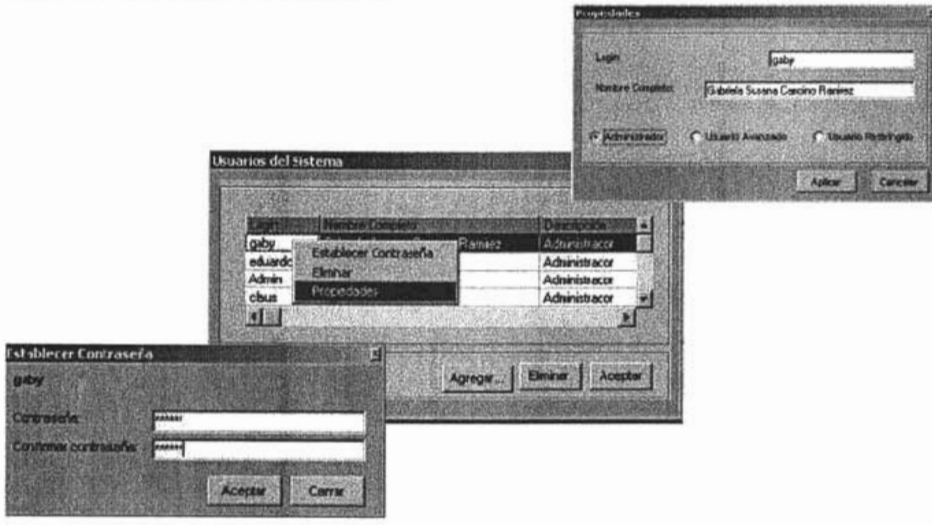


Figura 3.34 Pantallas de Usuarios del Sistema

Este formulario otorga al administrador la capacidad para agregar, modificar y eliminar información de los usuarios que pueden ingresar y administrar el sistema SAPPE.

3.4.3 Interfaz para Comunicaciones

Esta interfaz tiene el objetivo de brindar, a los usuarios enfocados a la operación y administración del hardware, una herramienta que facilite estas actividades de una manera transparente y sencilla. Para ello definimos la interfaz con base a dos necesidades básicas:

- Por una parte la operativa, es decir poder manipular y administrar los dispositivos conectados al sistema; Y por otra parte un contenido informativo que proporcione al usuario un seguimiento total sobre el comportamiento y condición actual del sistema.

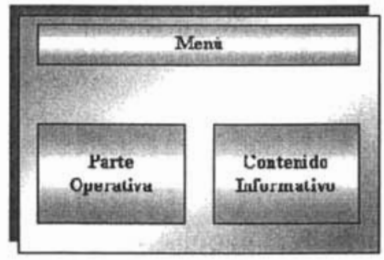


Figura 3.35 Elementos de Interfaz de Comunicaciones

Asimismo las políticas de seguridad implican un control de emergencias de operación del sistema de seguridad, es decir, un grupo de usuarios que tengan la capacidad de determinar las acciones a seguir una vez que se suscita un evento extraordinario, pueda reestablecer el estado normal del sistema y controle los distintos horarios de operación de los dispositivos.

Por lo tanto el contenido de la interfaz debe cubrir, por un lado, las expectativas de los administradores del hardware, y por otra parte facilitar a los administradores del sistema el control sobre su operación.

La solución fue una interfaz completamente gráfica, donde cada dispositivo del sistema es representado en la pantalla de manera virtual informando al usuario sobre su estado funcional y operativo así como su ubicación física.

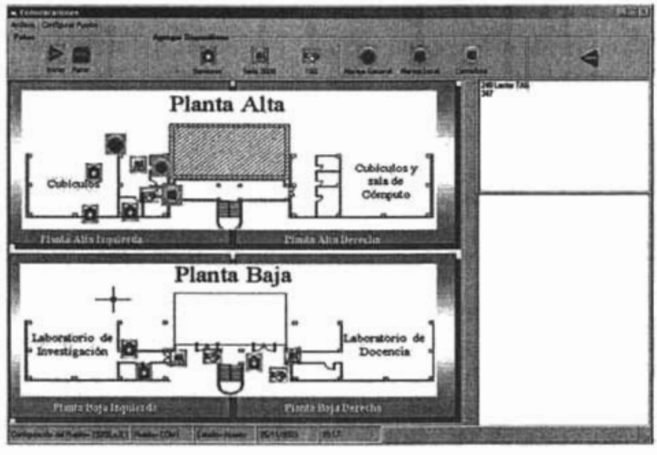


Figura 3.36 Pantalla Principal de Interfaz de Comunicaciones

Esta concepción del sistema permite al administrador del hardware:

- Configurar el puerto de comunicaciones.
- Instalar y desinstalar fácilmente un dispositivo.
- Realizar pruebas particulares, por área y generales de los dispositivos instalados en el sistema.
- Una rápida ubicación de fallas en los dispositivos.
- Seguimiento total sobre el comportamiento y condición actual del sistema.

Y permite al administrador del sistema:

- Configurar los horarios de operación de los dispositivos instalados.
- Visualizar fácilmente el área y el dispositivo que esta detectando un evento irregular.
- Restituir el estado de operación normal del sistema.

La interfaz gráfica del módulo de comunicaciones esta distribuido en tres partes principales:

- Menús
- Mapa virtual de la instalación. (Parte Operativa)
- Monitoreo de la operación de los dispositivos.

3.4.4 Menús

Los menús tienen el objetivo de brindar al usuario opciones más específicas como son la configuración del sistema y la administración de los dispositivos.

Esta pantalla ofrece un menú colgante con el cual el usuario podrá entrar a la configuración del puerto de comunicaciones. Una vez seleccionada la opción se despliega un formulario donde se presentan todos los parámetros que el usuario podrá manipular para realizar la comunicación con los dispositivos vía puerto serie.

Figura 3.37 Pantalla con Menú Colgante para Interfaz de Comunicaciones

Posterior a este menú se presenta una colección de botones caracterizados por íconos que permiten, por un lado, establecer la comunicación con los dispositivos y ,por otro lado, agregar nuevos dispositivos al sistema. Para ello el diseño de los íconos fue muy cuidadoso de manera que fueran expresivos y fáciles de relacionar con la operación correspondiente permitiendo al usuario habituarse a su utilización rápidamente.

Figura 3.38 Menú de íconos de la Interfaz de Comunicaciones

3.4.5 Mapa Virtual de la Instalación (Parte Operativa)

El mapa virtual permitirá, tanto a los administradores del hardware como a los administradores del sistema, asociar cada uno de los dispositivos físicos con un objeto representado en la pantalla, de manera que pueda reconocer el tipo de dispositivo, la ubicación física que ocupa dentro de las instalaciones y el estado actual del dispositivo; así como su dirección lógica, información útil para los administradores del hardware, que se puede obtener al posicionar el puntero del mouse sobre el objeto.

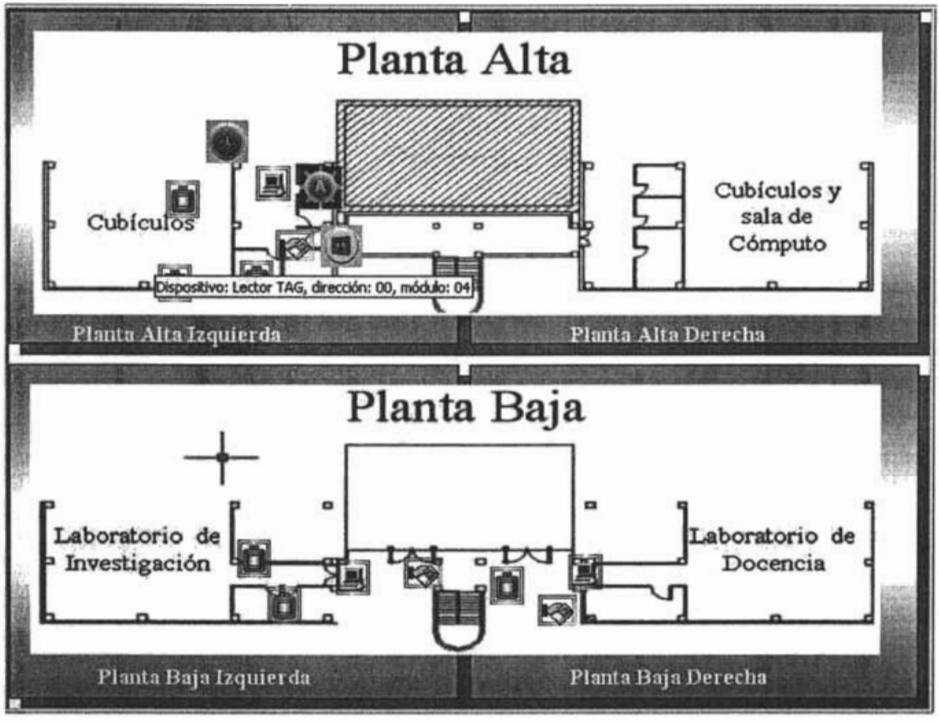


Figura 3.39 Pantalla del Mapa Virtual de las Instalaciones

Otra gran ventaja del mapa virtual es que el usuario podrá identificar rápidamente la zona y el dispositivo que haya detectado una situación anormal, ya que el objeto será resaltado mediante un color distinto, y podrá ser restaurado a su estado normal con sólo dar un clic sobre el elemento activo.

Contenido Informativo

La información presentada en esta pantalla la definimos de acuerdo con los intereses del usuario, es decir, seleccionamos aquella información que sería útil para el administrador del hardware. Mostrando en pantalla un seguimiento de los procesos que se están ejecutando entre el software y los dispositivos centrales:

- Transmisión de datos y respuesta
- Recepción de datos y acción tomada.
- Visualización de fallas en los dispositivos.

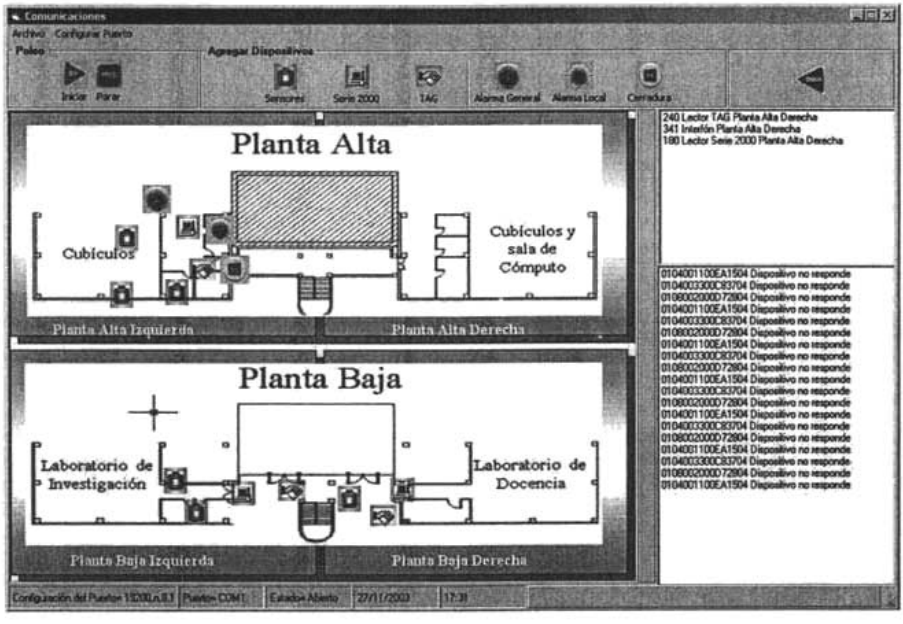


Figura 3.40 Pantalla con seguimiento de procesos de los dispositivos de hardware

3.5 Seguridad en el acceso de información

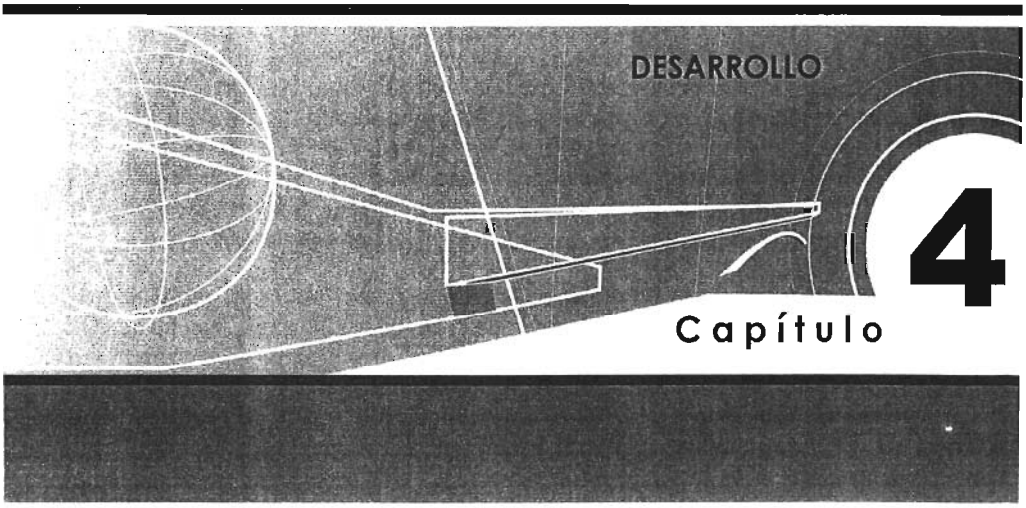
En términos operativos el sistema SAPPE es una aplicación orientada a procurar la seguridad de bienes y personas, esto implica todos los procesos que controlan los elementos de protección física. Sin embargo, existe un nivel de seguridad más abstracto que considera los elementos humanos como un factor importante para garantizar que se lleven a cabo todos esos procesos de manera exitosa.

Un sistema será mucho más seguro entre menor sea el número de usuarios que tengan acceso a él. Por ello determinamos que la administración del sistema fuera exclusiva de usuarios facultados y restringidos por distintos niveles de interacción con el software.

Estos niveles de interacción van a determinar la capacidad del usuario para hacer modificaciones y consultas dentro del sistema. Definimos tres tipos de usuarios y los privilegios otorgados para cada uno de ellos, como veremos en la siguiente tabla:

Usuario Restringido	Este tipo de usuario, tiene acceso a gran parte de las interfaces del programa, pero su interacción únicamente se limita a un nivel informativo; por ejemplo puede consultar toda la información concerniente a las Entradas/Salidas de usuarios, incluso acceder a detalles pero los procesos de manipulación de información estarán deshabilitados, este usuario no puede modificar y mucho menos borrar registros.
Usuario Avanzado	Este tipo de usuario estará autorizado para realizar consultas y manipular la información de manera limitada como puede ser: restringir accesos, permitir salidas de equipo, etc. Adicionalmente puede restaurar el sistema a su estado normal después de algún evento extraordinario.
Administrador	Tiene pleno control sobre todas las capacidades y funcionalidades de la aplicación y la Base de Datos. Cabe destacar que este usuario también tendrá decisión sobre los otros dos tipos de usuario. Operativamente el administrador es el encargado de crear e eliminar los otros dos tipos de usuario, decidir quién tendrá permisos de usuario restringido, quién de avanzado, además de tener capacidad para asignar y cambiar nombres de usuario y contraseñas en cualquier momento.

Tabla 3.1 Usuarios y Privilegios


DESARROLLO
Capítulo
4

Capítulo

4

DESARROLLO

4.1 El Desarrollo

En esta etapa generamos un sistema que ejecutara todas las funciones definidas durante el diseño. Consideramos que el diseño y desarrollo son procesos estrechamente ligados, por lo que aún cuando en el diseño obtuvimos una aplicación que cumpliera con las funciones del sistema, recurrimos en algunos módulos al rediseño de sus algoritmos y adición de funciones que hicieran más eficiente su operación e incrementaran las capacidades y velocidad del sistema.

En SAPPE los eventos van a controlar el curso de la aplicación, de modo que, con la ocurrencia de un evento se ejecutará la función o procedimiento asociado a ese evento. La aplicación siempre estará a la espera de un evento, lo que implica que ciertas partes de código podrán ejecutarse una vez, varias veces o bien nunca ejecutarse. Los eventos serán provocados por las acciones externas que ejecuta el usuario sobre el programa (por ejemplo el movimiento del Mouse), o bien por acciones internas en respuesta al proceso entre la aplicación y el hardware.

Como mencionamos anteriormente, Seleccionamos Visual Basic 6.0 como nuestro entorno de programación ya que es un lenguaje visual, interactivo y orientado a eventos.

Para potenciar las capacidades del programa utilizamos el sistema administrador de Bases de Datos InterBase a través del cual nos solo tenemos un rápido acceso a los datos, sino que además nos permitió generar código que disminuyera la carga en muchos procesos de la aplicación.

Siguiendo la estrategia del apartado de diseño, desglosaremos los procesos principales de cada modulo para describir su traducción a un código ejecutable. Básicamente en el desarrollo los módulos que realizan las operaciones lógicas y funcionales del sistema son: Comunicaciones y Bases de Datos, puesto que de ellas depende el correcto funcionamiento del sistema.

4.2 Bases de Datos

Durante la etapa de diseño construimos un esquema conceptual de la información implicada en el sistema definiendo los tipos de datos, las tablas y sus relaciones. En esta etapa describiremos los procedimientos almacenados utilizados para realizar consultas automatizadas con el objetivo de disminuir tiempos de proceso dentro de la aplicación.

Básicamente estos procedimientos están orientados a realizar la validación de datos tales como números de identificación de tarjetas de usuario, números de identificación de chips para protección de equipo y horarios establecidos para los dispositivos del sistema de seguridad.

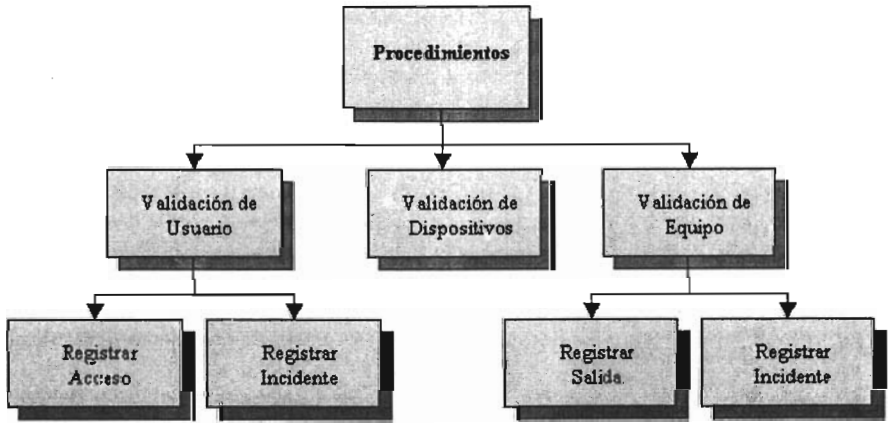


Figura 4.1 Procedimientos almacenados en la Base de Datos

Validación de Usuario

Este procedimiento permite a la aplicación definir si el usuario esta o no autorizado para entrar a las instalaciones. Una vez realizada la lectura de la tarjeta del usuario se realiza una comparación del número de identificación contra los registros de la base de datos para comprobar:

- Que exista el usuario.
- Que tenga autorización de acceso.

- Que el ingreso sea dentro del horario, día y fecha especificado para el usuario.

- Que el ingreso sea dentro de las áreas permitidas para el usuario.

Después de realizar la identificación del usuario se ejecuta uno de los siguientes procedimientos:

- Registrar Acceso Usuario. Si el usuario tiene autorización de entrada se registra la hora y fecha de acceso así como el área a la que está ingresando.

- Registrar Incidente Usuario. Si el usuario no tiene autorización de acceso se registra en los incidentes del usuario la hora, fecha y descripción del incidente ocurrido.

(Ver Anexo C Figura 1, 2 y 3 para conocer los procedimientos de Usuario)

Validación de Equipo

Este procedimiento va a facilitar al sistema el control de la salida de los equipos de las instalaciones. Una vez que la aplicación detecte un dispositivo de equipo se realizará una comparación entre el número de identificación del chip del equipo contra los registros de la Base de Datos para determinara que:

- El equipo tenga autorización de salida.

- El equipo salga dentro del horario y fecha especificados.

Inmediatamente después de realizar la comparación se ejecutará uno de los siguientes procedimientos:

- Registrar Salida Equipo. Si el registro tiene autorización de salida y es extraído dentro del horario y fecha definidos por el responsable del equipo se creará un registro con los datos del equipo, la hora y fecha de salida.

- Registrar Incidente Equipo. En caso de que el equipo no esté autorizado para salir o salga fuera del horario y fecha definidos se creará un registro detallando el incidente, la hora y fecha en que ocurrió.

(Ver Anexo C Figura 4, 5 y 6 para conocer los procedimientos de Equipo)

Validación de Dispositivos

La validación de dispositivos facilita al programa el monitoreo del hardware confirmando los horarios y fechas de operación definidas para cada elemento del sistema. Al ejecutar dicho procedimiento se comparará el identificador lógico del dispositivo contra los registros de la Base de Datos para identificar si el dispositivo:

- Tiene restricción de horario
- En caso de tener restricción comprobar el horario y fecha actuales contra el horario y fecha determinados para el dispositivo

de manera que al ejecutar dicho procedimiento la aplicación pueda definir:

- Si debe o no comprobar el estado actual del dispositivo
- Si debe activar una alarma.

(Ver Anexo C Figura 7 para conocer los procedimientos de Dispositivos)

4.3 Comunicaciones

El módulo de comunicaciones va a ejecutar los procesos críticos del sistema. Es precisamente en este módulo donde se va a dar seguimiento a las operaciones de seguridad tales como:

- Transmisión, captura y procesamiento de datos entre la computadora y los equipos electrónicos de seguridad.
- Validación de la información recibida mediante la base de datos.
- Recopilación de la información del incidente ocurrido y evaluación de las acciones correspondientes.
- Generación de los mensajes de alerta.
- Resolución y ejecución de las acciones de emergencia definidas.
- Recopilación de la información de los incidentes ocurridos.

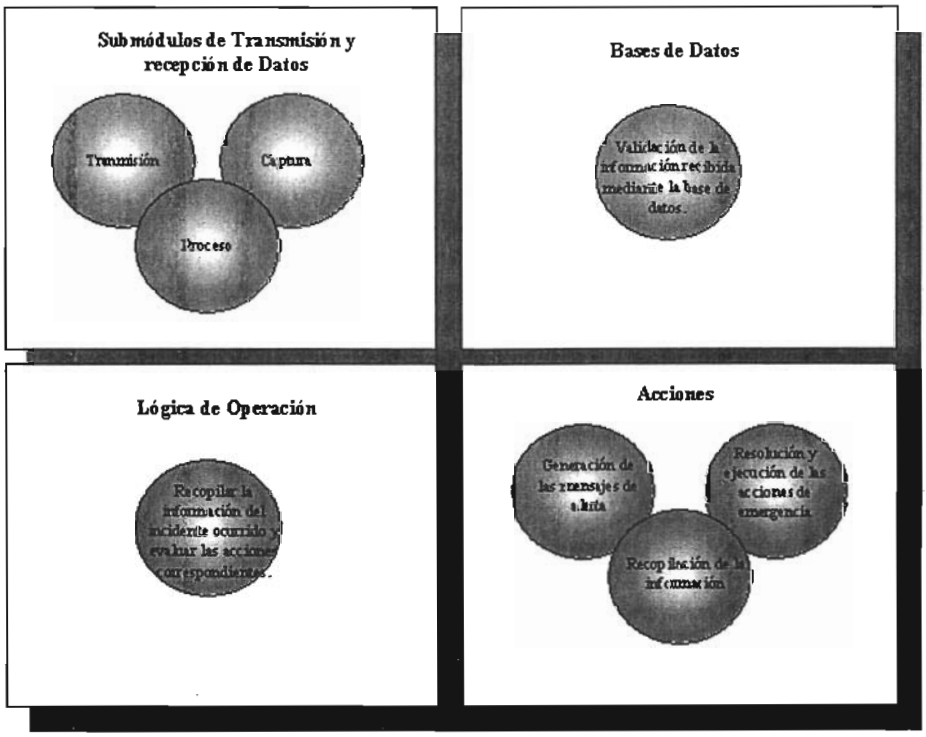


Figura 4.2 Principales funciones del módulo de comunicaciones

Por ello es de suma importancia que cada una de las funciones implementadas opere de forma óptima, asegurando que la aplicación cumpla con los objetivos principales del sistema de seguridad.

En la figura 4.2 podemos ver las principales funciones del módulo de comunicaciones organizadas con base en los criterios definidos durante la etapa de diseño. A continuación detallaremos cada una de ellas describiendo su lógica operativa.

Submódulos de transmisión y recepción de Datos

La principal función de la aplicación en esta etapa es coordinar la comunicación entre la computadora y el hardware. La computadora representa el maestro y los dispositivos conectados al sistema fungen como esclavos que únicamente responden a las peticiones realizadas por el maestro.

Para lograr la sistematización de los datos implementamos un protocolo basado en el estándar RS-232 ,que nos permitió realizar la comunicación entre la aplicación y el puerto serie de la computadora, y el Tiris Bus Protocol , a través del cual los comandos enviados a los dispositivos serían comprendidos por éstos y sus respuestas interpretadas por SAPPE V.0.

La sincronización de los datos así como las operaciones de codificación y decodificación de las cadenas se ejecutan por una función principal que se encarga de recorrer en forma cíclica cada dispositivo conectado al sistema enviando instrucciones de lectura para valorar el estado actual del dispositivo y posteriormente decodificando la respuesta obtenida de esta acción (ver figura 4.3).

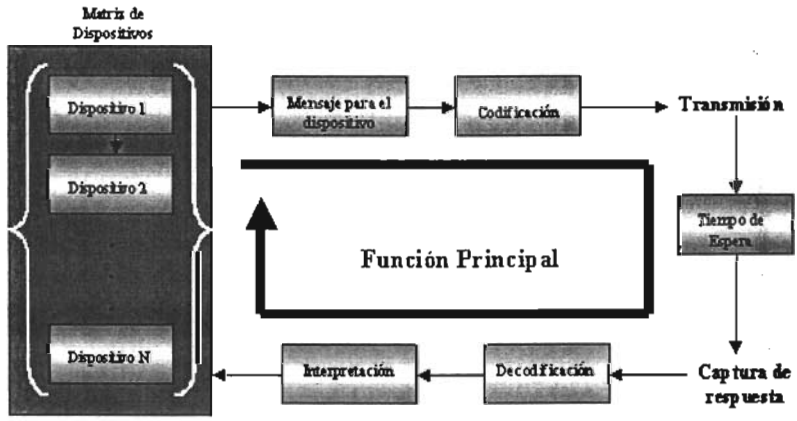
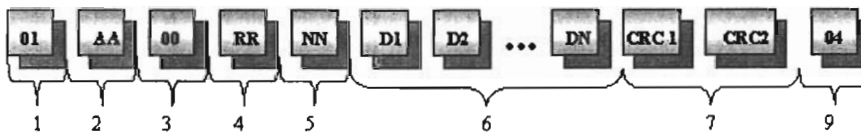


Figura 4.3 Función principal del Sistema SAPPE

Estructura del mensaje.

El formato que debe seguir la instrucción enviada para que pueda ser comprendida por el dispositivo de acuerdo al Tiris Bus Protocol debe contener la siguiente estructura:



Inicio de trama

Dirección destino

Dirección origen

Código de instrucción

Longitud de mensaje

Mensaje

Código de detección de errores

Fin de trama

Figura 4.4 Estructura del mensaje basado en el Tiris Bus Protocol

Una parte fundamental del mensaje es el Código de Detección de Errores (CRC) el cual va a comprobar que la información recibida es correcta, para ello existen muchos códigos para el control de errores. Tiris Bus Protocol utiliza CRC-CCITT[1] un algoritmo que utiliza un "número mágico" (valor) que permite generar la cadena de detección de errores, este número mágico no es único, cada protocolo de comunicación determina su valor, por lo que resultó sumamente complejo poder

[1] Conocido como Código de Redundancia Cíclica, es un algoritmo de detección de errores basado en un polinomio. (10001000000100001 = X^16 + X^12 + X^5 + 1) . Básicamente se genera añadiendo a la cadena a enviar un dato adicional cuyo valor se calcula a partir de los datos del mensaje principal. Esta nueva cadena se envía al receptor quien se encarga de descomponer la cadena principal del CRC transmitido, de manera que pueda recalcular el CRC recibido y compararlo contra el CRC transmitido; si ambos coinciden se verifica que los datos recibidos son correctos en caso contrario se solicita la retransmisión del mensaje.

generar el algoritmo que utiliza el Tiris Bus Protocol. Como solución alterna el Tiris Bus Protocol puede usar otro algoritmo más fácil de implementar: el XOR.
Su implementación tanto en Visual Basic como en el microprocesador del dispositivo lector resultó una opción más adecuada, por lo que optamos por este algoritmo.

Codificación del Mensaje

Los datos de la cadena generada deben ser dirigidos en código Hexadecimal a los dispositivos, sin embargo el puerto serie interpreta la información en código ASCII, por lo que requerimos hacer conversión de datos para lograr que los dispositivos recibieran la información de modo congruente con la comunicación establecida por el Tiris Bus protocol.

Visual Basic no cuenta con instrucciones de conversión directa entre código Hexadecimal y ASCII, sin embargo puede realizar conversiones de valores Decimales a valores en ASCII, lo que sugirió una transformación alterna de los valores Hexadecimales a Decimales y posteriormente de valores Decimales a equivalentes ASCII.

Cada mensaje enviado o transmitido esta formado por una secuencia de caracteres agrupados de dos en dos. Los algoritmos de conversión utilizan parejas de caracteres para la interpretación de datos.

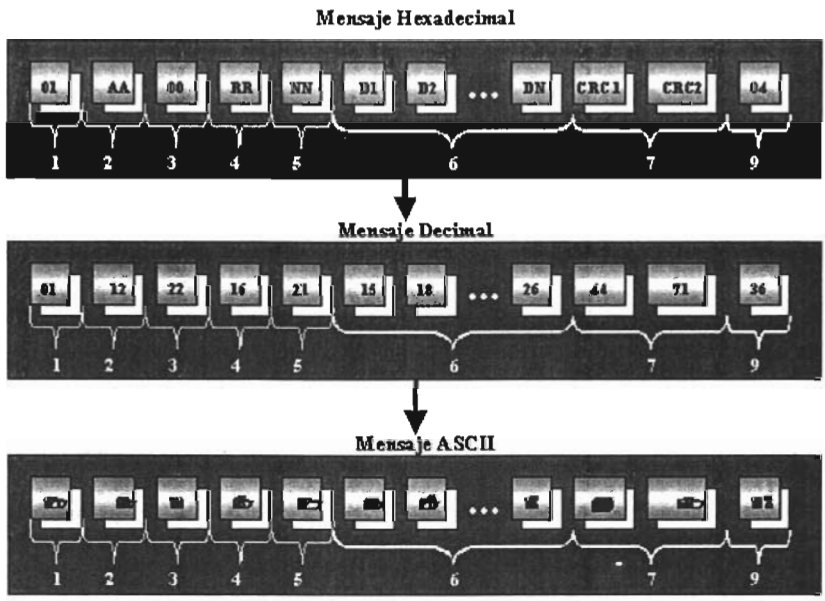


Figura 4.5 Proceso de codificación del mensaje

Tiempo de Espera

Durante el proceso de transmisión es necesario considerar un tiempo de espera antes de liberar el mensaje para el siguiente dispositivo, con el objetivo de asegurar que el bus de comunicación ha quedado libre de la transmisión anterior. De igual forma el recorrido de los datos a través del bus de comunicaciones hasta el módulo de control de los dispositivos, la respuesta de estos mismos y el retorno de los datos al puerto serie implica un tiempo de retardo que varía de la distancia entre los dispositivos y la computadora, y de la velocidad de transmisión establecida por el protocolo de comunicación. Estos tiempos de retardo y espera son de suma importancia ya que si no se toman en cuenta se pueden producir errores de comunicación como colisión y pérdida de datos.

Velocidad	Tiempo de byte (10 bits)	Tiempo de byte (11 bits)
2400 bps	4.167 ms	4.583 ms
4800 bps	2.083 ms	2.292 ms
9600 bps	1.042 ms	1.146 ms
19200 bps	0.521 ms	0.573 ms
38400 bps	0.260 ms	0.286 ms
57600 bps	0.174 ms	0.191 ms
115200 bps	0.087 ms	0.095 ms

Tabla 4.1

Decodificación del mensaje

De manera recíproca a la codificación de mensajes, los datos recibidos del hardware llegan al puerto serie en una secuencia de caracteres en ASCII los cuales deben ser convertidos a valores Hexadecimales para interpretar la respuesta generada por los dispositivos. Por lo que el proceso de decodificación implica una conversión de valores ASCII a Decimales y Decimales a Hexadecimales.

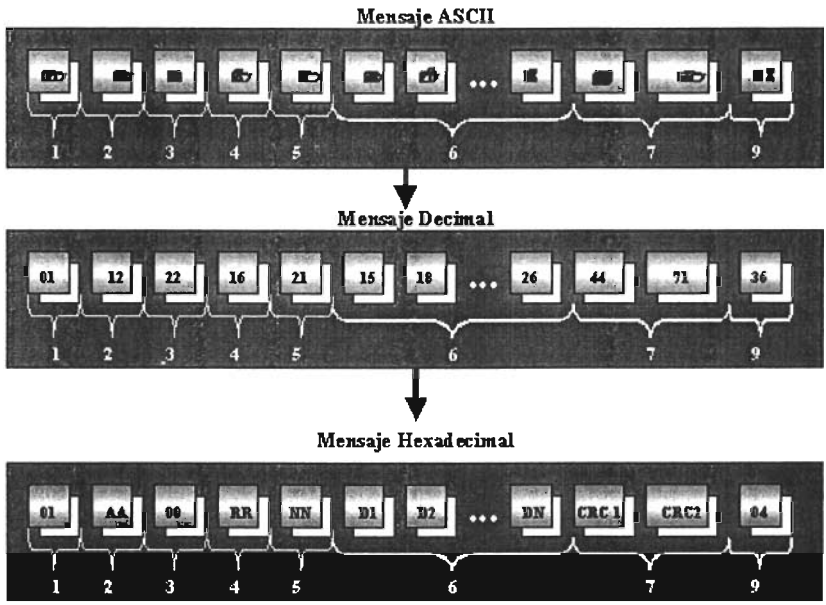


Figura 4.6 Proceso de decodificación del mensaje

Una vez realizada la decodificación de la información recurrimos a un proceso de descomposición de la cadena, de manera que podamos interpretar los datos recibidos, utilizando para ello la estructura definida para la construcción de los mensajes.

4.4 Validación de Información

Sin duda la protección física de los individuos y equipos registrados, es la parte más importante del sistema de seguridad, ésta sólo se puede lograr mediante la validación de los mismos a través de un identificador único; es precisamente en este punto donde intervienen los dispositivos de radiofrecuencia en interacción con el sistema SAPPE V.0 y más profundamente con la Base de Datos.

La Base de Datos nos va a permitir establecer condiciones particulares para cada persona y equipo que deseen ser resguardados, estas condiciones van a definir las restricciones con las cuales el usuario podrá acceder a las instalaciones y los equipos podrán ser extraídos o desplazados.

Asimismo mediante la Base de Datos se podrán almacenar las características de operación de cada uno de los dispositivos electrónicos de detección (como son los sensores magnéticos, de movimiento y ruptura de cristales), de manera que brinde al administrador del usuario la capacidad para determinar en que momento desea activar o desactivar la operación de alguno de ellos.

De acuerdo con estas consideraciones la Base de Datos nos va a proporcionar la información necesaria para validar:

- Usuarios
- Equipo
- Dispositivos electrónicos de detección.

De modo que al recibir el mensaje como respuesta de la interacción software-hardware el siguiente proceso quedará definido por la comparación del dato recibido contra la información contenida en la base de datos, como podemos ver en la siguiente figura (Figura 4.7).

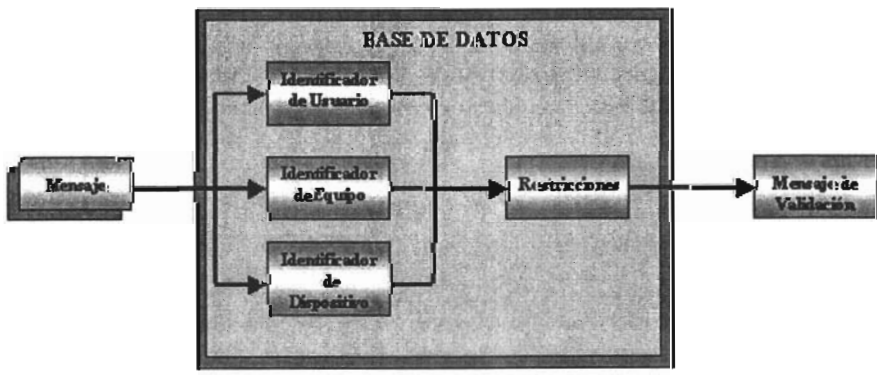


Figura 4.7 Proceso de validación entre el software y la Base de Datos

4.5 Lógica de Operación

La lógica de operación va estrechamente ligada con el proceso de validación de la información. A través de esta lógica podremos evaluar los resultados obtenidos de la comparación del mensaje con la Base de Datos, para determinar el grado de peligro y las acciones de emergencia que deberán ser tomadas.

Para poder realizar este proceso es necesario poder identificar desde el momento de la transmisión y recepción de datos que dispositivo es al que estamos llamando y cual es su ubicación física, de manera que podamos decidir con que criterios habremos de evaluarlo y cuales serán las acciones correspondientes.

Para ello, como habíamos mencionado anteriormente, utilizamos una matriz de dispositivos los cuales serán recorridos de manera cíclica para estar verificando su condición actual. Esta matriz esta formada por cadenas que se construyen al iniciar o actualizar la aplicación, y que llevan en su estructura la información necesaria para poder determinar el tipo de dispositivo, su dirección lógica, su ubicación física y las instrucciones de operación.

La matriz tiene una dimensión de **n** Renglones por **2** Columnas, en donde cada renglón representa un dispositivo, la columna 1 determina las características del dispositivo y la columna 2 la instrucción en código ASCII[2] que será transmitida (Ver Figura 4.8).

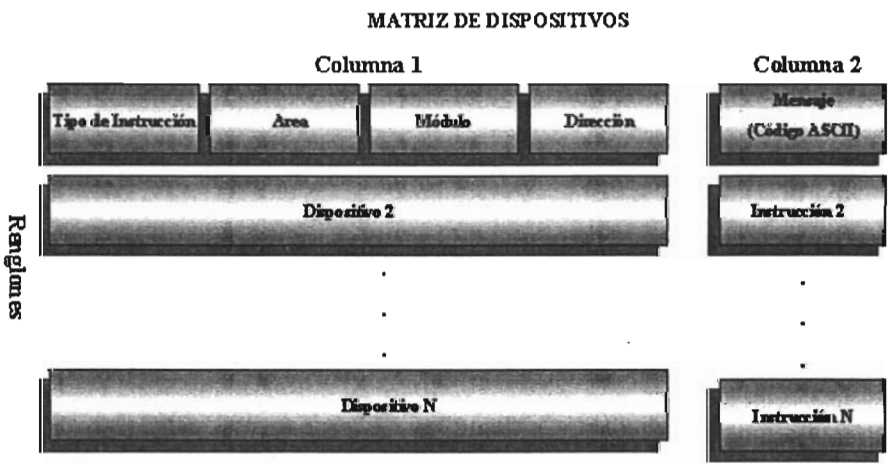


Figura 4.8 Estructura de la matriz de comprobación de dispositivos

[2] Desde el momento en que se genera la matriz se va convirtiendo cada instrucción Hexadecimal a código ASCII, de manera que disminuya el tiempo de proceso de la transmisión de datos, al realizar la conversión una sola vez al iniciar la aplicación .

Tipo de instrucción

Existen tres tipos principales de dispositivos clasificados de acuerdo al tipo de instrucción que debe ser enviada para manipularlos. Cada uno de estos tipos de dispositivos utiliza un código de lectura de datos distinto, maneja un nivel de frecuencia diferente y se enfoca a la captura de un tipo de información específica. Por lo que, al incluir información de éstos en la matriz de lectura , decidimos distinguirlos por sus iniciales para poder interpretar de manera correcta sus respuestas:

1. "S2" (Serie 2000) Destinado para la identificación de equipo.
2. "TG" (TAG) Destinado para la identificación de usuarios.
3. "SN" (Sensores) Dispositivos electrónicos de detección.

Área

El área nos va a permitir determinar durante la ocurrencia de un evento su posición específica, de modo que al ejecutar la acción correspondiente podamos dirigirla a la zona correcta.

El área esta determinada por un índice numérico que se puede incrementar conforme se adicionen áreas al sistema, esta característica permitirá una aplicación con mayor flexibilidad y capacidades de crecimiento a largo plazo.

1 – Planta Alta Derecha
2 – Planta Alta Izquierda
3 – Planta Baja Derecha
4 – Planta Baja Izquierda

Módulo y Dirección.

Un módulo es el dispositivo controlador que se encarga de recibir y transmitir la información que lee a través de su antena. Cada módulo cuenta con ocho puertos físicos que permiten la conexión de los dispositivos de detección electrónica y dispositivos de acción, los cuales pueden ser controlados por medio de él.

Los parámetros de dirección de módulo y dirección de dispositivo están formados por dos caracteres hexadecimales que definen la ubicación lógica y física que tiene el dispositivo dentro del hardware (p. Ej. 01, FF). La dirección del módulo indica el nombre lógico del emisor-receptor de datos donde se encuentra conectado el dispositivo, y la dirección del dispositivo indica la dirección física del puerto que esta utilizando dicho dispositivo, dentro del módulo.

Con esta información podemos manipular los dispositivos, obtener e interpretar sus respuestas contrapuestas con la Base de Datos y conocer el área dónde se está manifestando un suceso anormal, sin embargo para poder dar seguimiento al

evento debemos saber que dispositivo, de una manera más específica, está detectando la información de alerta. Esto nos va a permitir catalogar la gravedad del incidente y determinar la acción de emergencia que se llevará a cabo. Para ello consideramos los siguientes puntos:

- Existen dispositivos dedicados a la captura de información con características similares como son dirección de módulo, dirección específica, área, etc.

- Existen dispositivos dedicados a desencadenar eventos como son activación de alarmas, apertura y cierre de puertas, a los que llamamos actuadores.

Derivando de estos puntos decidimos crear dos tipos de objetos que nos permitieran manipular su información de una manera más directa y particular: *dispositivos de lectura y actuadores*, cada uno de ellos con propiedades que definen su identidad (Véase Fig. 4.9).

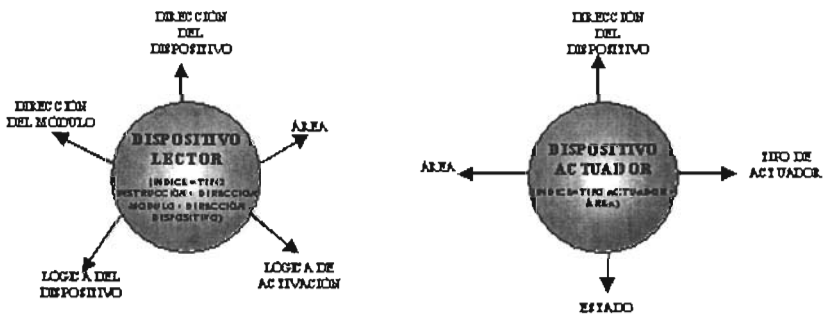


Figura 4.9 Tipo de objetos creados para manipular los equipos

Índice del Tipo de Objeto

El índice del tipo de objeto nos va a permitir enumerar cada uno de los dispositivos cargados durante la ejecución del programa, de manera que al hacer referencia a alguno de ellos podamos obtener sus propiedades.

Cada uno de estos tipos responde a un índice particular formado por los siguientes parámetros:

- Tipo de instrucción + Dirección de módulo + Dirección del Dispositivo (Para el dispositivo lector)

- Tipo de Actuador + Área (Para el dispositivo actuador)

En el caso del dispositivo lector utilizamos características que habíamos definido anteriormente como son su dirección física y lógica, los cuales se encuentran determinados en código Hexadecimal, pero para este propósito fueron convertidos en código Decimal. De esta forma un dispositivo con las siguientes características: "Sensor de Movimiento" con dirección "08" en el módulo "01"; podemos referirlo como tipo de objeto "SN"=3, Dirección de Módulo=1 y Dirección de Dispositivo= 8 lo que origina el índice numérico 3+1+8 (318) dentro de la aplicación.

En el caso del dispositivo actuador el parámetro tipo actuador lo definimos de la siguiente manera:

1. Cerradura Magnética (Para la apertura y cierre de puertas)

2. Alarma Local (Para dar aviso sobre incidentes menores como puertas abiertas)

3. Alarma General (Para alertar sobre los incidentes de mayor emergencia como el robo de equipo)

Como ejemplo de este tipo de objeto si tuviéramos un actuador "Cerradura Magnética" que se encuentra en la Planta Alta Derecha tendríamos "Cerradura Magnética" = 1 + "Planta Alta Derecha" = 1, lo que daría por resultado un objeto cuyo índice numérico es 11.

Propiedades del Tipo de Objeto

Como observamos en la figura 4.18, cada tipo de objeto está descrito por una serie de parámetros que lo hacen único, principalmente su dirección física, la dirección del módulo donde se encuentran conectados y la ubicación que ocupan dentro de las instalaciones. Estos parámetros ya han sido definidos anteriormente, sin embargo, existen otras características que aportan al sistema información importante para su correcto manejo dentro de la aplicación.

Por una parte es necesario conocer específicamente el propósito y modo de operación de cada uno de los dispositivos lectores conectados al sistema, de manera que facilite la determinación de los estados de emergencia y acciones que se deben llevar a cabo en cada caso.

Para ello definimos una *Lógica del Dispositivo* la cual clasifica a los dispositivos lectores de la siguiente manera:

1. Serie 2000 (Protección de Equipo)
2. Lector TAG (Protección de personal)
3. Sensor de Movimiento (Detectan movimiento en un rango de área).
4. Sensor de Ruptura (Protección de Ventanas)
5. Sensor Magnetico (Protección de entradas de acceso a personal)
6. Interfon (Notificador de accesos de personal no registrado)
7. Boton Emergencia ((Actúa durante contingencias como sismos, incendios, etc.)
8. Sensor Magnético (Protección de Entradas de Acceso y Salida de Equipo)

Los dispositivos de detección electrónica (Sensores y Botón de Emergencia) operan bajo dos estado de voltaje que se traducen en "0" y "1", de modo que uno de estos niveles indica su condición normal y el otro su condición de emergencia. Para distinguir este modo de operación definimos una **lógica de activación** la cual puede ser positiva o negativa, de acuerdo con lo siguiente:

- Positiva (1). Si el dispositivo transmite "0" cuando opera normalmente y "1" si detecta un estado de emergencia.
- Negativa(0). Si el dispositivo transmite "1" en estado normal y "0" en estado de emergencia.

Por otra parte al dispositivo actuador adicionalmente a las características definidas anteriormente (dirección del dispositivo, área y tipo de actuador) agregamos un valor que permitiera al programa saber en que momento el sistema se encontraba en estado de emergencia. Para ello el **estado** del actuador actúa como una bandera que se activa durante un evento y se mantiene así hasta que el sistema es reestablecido; garantizando de esta forma que las acciones de seguridad ejecutadas por el sistema se mantengan vigentes hasta que una persona autorizada tome el control del suceso.

4.6 Acciones

Las acciones son la culminación del complejo proceso que hemos ido desglosando a lo largo de este capitulo y que permiten llevar a cabo de manera real el cumplimiento de las políticas de seguridad establecidas. Las acciones van inmersas en el proceso de evaluación y determinación de las acciones de emergencia, a través de ellas podremos ejecutar las actividades correspondientes a cada uno de los dispositivos involucrados en el evento extraordinario.

Una vez que se ha cuestionado, comparado y validado cada uno de los dispositivos estamos capacitados para dar una resolución y ejecutarla, así como dar seguimiento al incidente ocurrido con la recopilación de información del evento y la generación de avisos. (Figuras 4.10 y 4.11)

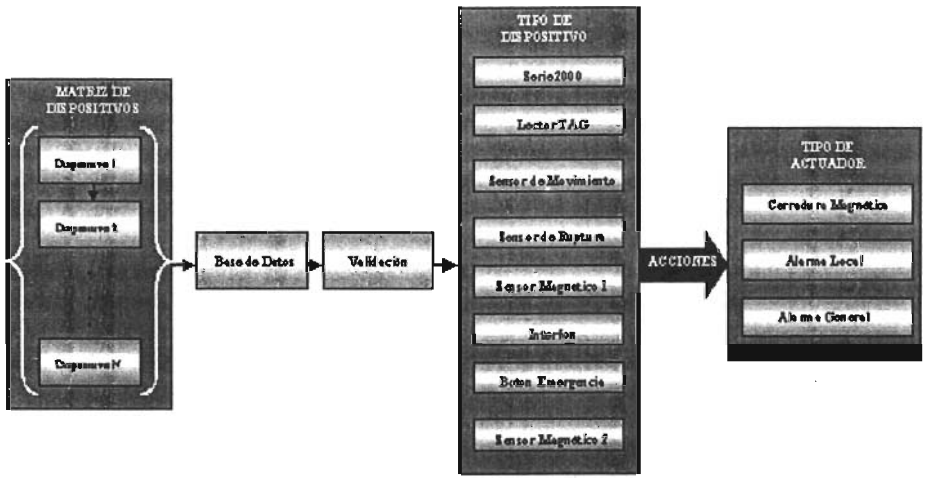


Figura 4.10 Proceso completo de comunicaciones. Las acciones determinan que dispositivo actuador será el que se activará en caso de una emergencia.

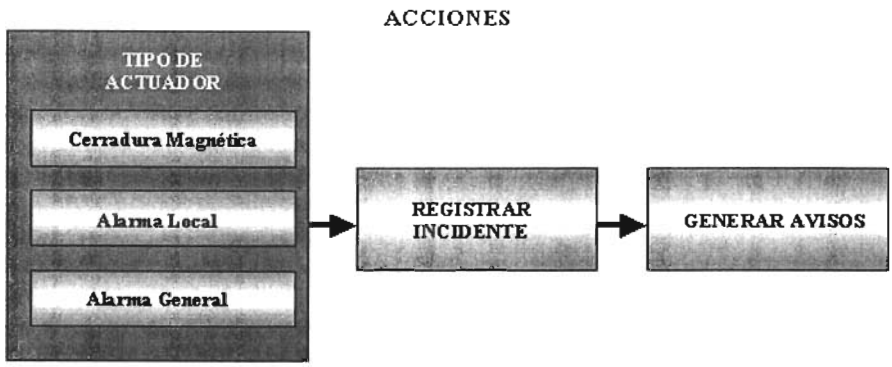


Figura 4.11 Funciones ejecutadas después de detectar un evento extraordinario

Selección del tipo de actuador

La primer función que se debe ejecutar después de determinar que un dispositivo se encuentra en estado anormal, es la selección del actuador que se debe accionar de acuerdo con la gravedad del evento ocurrido, para ello se generó una lógica de acción que responde todos los posibles incidentes que se pueden presentar como vemos en la siguiente figura (Figura 4.12).

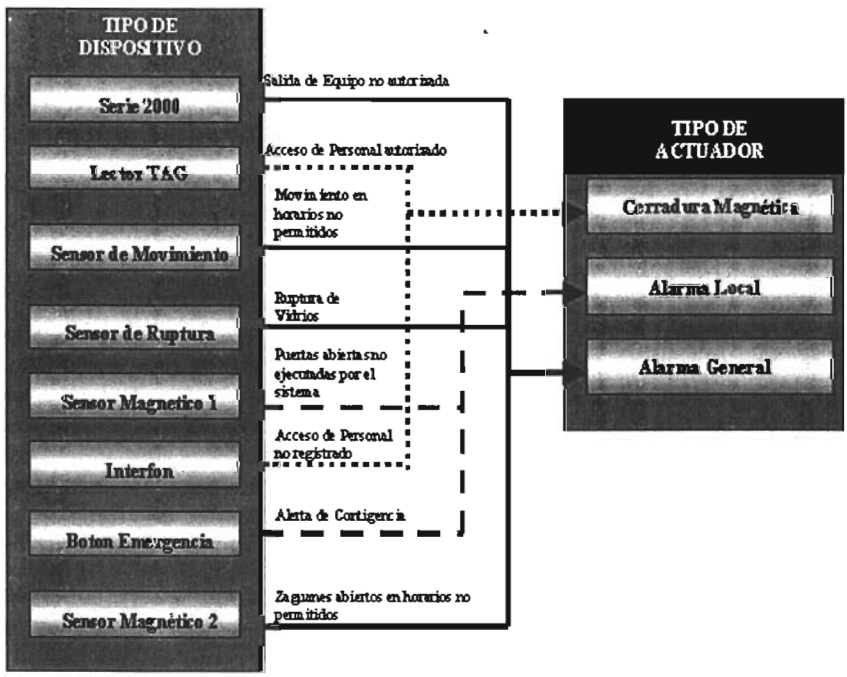


Figura 4.12 Selección del Tipo de Actuador

Registrar Incidente

La recopilación de información es una actividad indispensable en un sistema de seguridad, ya que a partir de ella se pueden administrar y cuantificar de manera exacta todos los incidentes ocurridos durante la operación del sistema.

Almacenar la información estratégica de los eventos extraordinarios ofrece al usuario una poderosa herramienta de control; por ello, después de determinar que ha ocurrido un incidente, decidimos capturar los datos relevantes del suceso en la base de datos con el objetivo de poder consultarlos posteriormente.

Consideramos que los datos que deben ser registrados son:

- Descripción del incidente. Obviamente es necesario saber que tipo de incidente fue el que se suscitó.
- Hora y fecha. Saber con exactitud el día y hora en que se presentó un evento permiten realizar análisis más profundos y búsquedas más específicas.
- Ubicación. Es importante informar sobre el lugar donde ocurrió el evento.

Generar avisos

La generación de avisos va a permitir al usuario estar al tanto de lo ocurrido desde el instante en que se da un evento, con lo que puede llevar a cabo una política de acción de forma inmediata sin tener que consultar los registros en la base de datos.

Para ello decidimos desplegar la misma información que se está registrando en la base de datos: descripción del incidente, hora, fecha y ubicación en una pantalla resaltada por colores llamativos y letras grandes.

4.7 Seguridad

Para acceder a la aplicación el usuario deberá contar con un nombre y una contraseña que valide sus privilegios dentro del sistema. Este proceso de validación debe realizarse herméticamente de manera que garanticemos que la información que inserte el usuario, y que se almacena dentro de la base, sea difícil de corromper o deducir.

Para ello generamos dos funciones de encriptación que almacenan la información del usuario de una forma totalmente distinta a la que ellos ingresan al sistema.

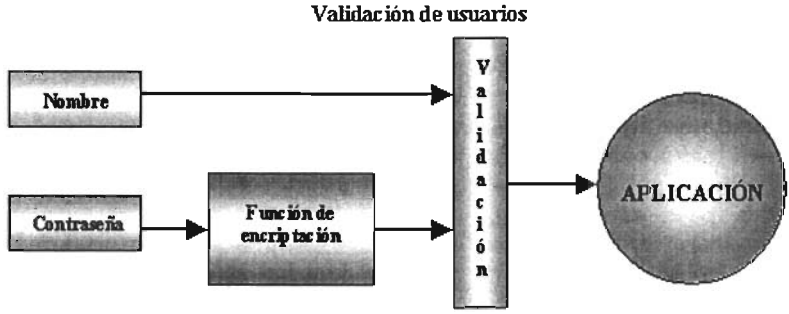
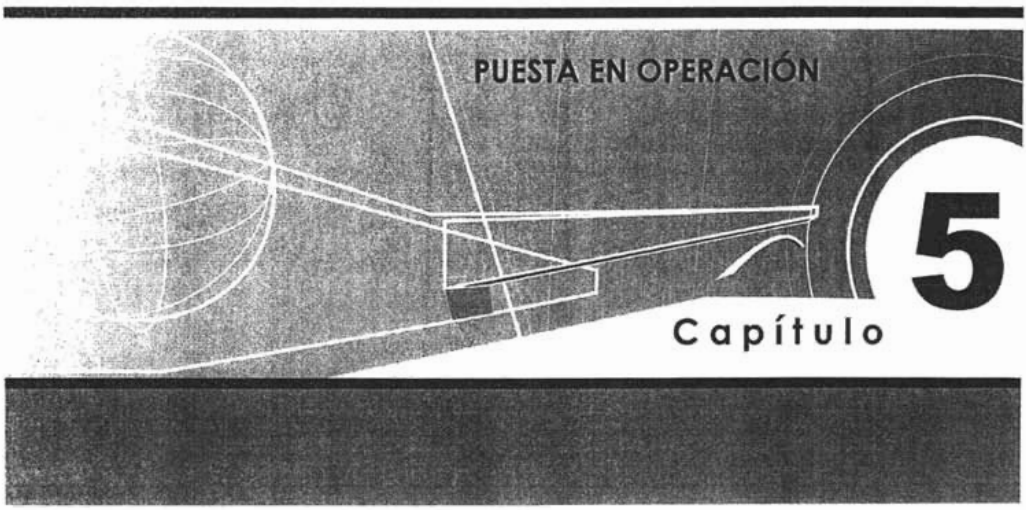


Figura 4.13 Proceso para la validación de usuarios de sistema


PUESTA EN OPERACIÓN
Capítulo
5

Capítulo

5

PUESTA EN OPERACIÓN

5.1 Estrátegia

Los procesos de implantación y pruebas constituyen la culminación del proyecto. Es la etapa más difícil ya que implica la integración de todos los procesos involucrados en el sistema y su confrontación con un ambiente real.

El sistema "Tarjetas Inteligentes" es un sistema cuya infraestructura se encuentra basada en tecnología reciente, por lo que su instalación y adaptación, al edificio y los usuarios, resultó una ardua tarea para todos los integrantes del proyecto que tuvimos que enfrentar grandes dificultades. Por ello, formulamos una estrategia de instalación que nos orientara durante este proceso poniendo extrema atención en todos los detalles:

- Armar e instalar los dispositivos electrónicos y componentes adicionales.
- Instalar y desplegar la versión final del software de aplicación. (SAPPE V.0)
- Realizar las pruebas finales de todos los elementos del sistema.
- Realizar los ajustes que resulten necesarios.
- Preparar la documentación necesaria, como manuales técnicos y de operación.
- Designar al personal que va a operar el sistema.
- Capacitar a los usuarios sobre el funcionamiento del sistema.
- Mostrar la operación del sistema a los usuarios.
- Darle mantenimiento al sistema.
- Asegurar que se cuente con fuentes alternas de energía.
- Operar el sistema durante un periodo de prueba.
- Evaluar la operación del sistema y tener reuniones informativas con los usuarios.
- Preparar propuestas para mejorar el sistema.
- Aplicar cualquier mejora aprobada.

De un modo más organizado y general clasificamos todos estos puntos en procesos que nos dieran una visión más clara de las actividades a realizar como podemos observar en el diagrama 5.1 que se muestra a continuación.

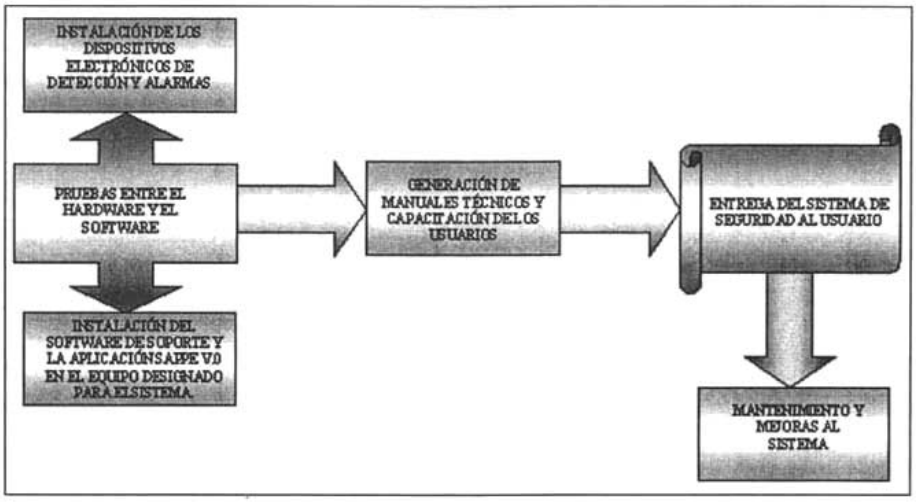


Figura 5.1 Procesos involucrados en la implantación del sistema

A partir de esta diagrama vamos a detallar todas las acciones realizadas para cada uno de los procesos:

5.2 Consideraciones para la instalación de los dispositivos electrónicos de detección y alarmas

La instalación física de los elementos del sistema de seguridad fue realizada por nuestros compañeros especializados en la parte electrónica, quienes de manera minuciosa distribuyeron estratégicamente los dispositivos electrónicos de detección y alarmas en las zonas más vulnerables del edificio, garantizando con ello una cobertura total de las instalaciones.

Para llevar a cabo el armado, conexión y cableado del hardware nuestros compañeros realizaron un análisis previo de todas las características que influirían de manera directa o indirecta en la instalación del sistema y su correcta operatividad. Para ello consideraron tres elementos principales:

- El entorno físico donde sería instalado el sistema.
- Los costos de inversión y mantenimiento del sistema.
- El elemento humano.

5.2.1 El entorno físico donde sería instalado el sistema

El Sistema "Tarjetas Inteligentes" es un proyecto robusto que combina distintas tecnologías para garantizar una protección total del usuario y sus bienes; el hardware utilizado para su implementación opera capturando variaciones electromagnéticas (como tarjetas inteligentes y chips de radiofrecuencia), eléctricas (como botones de emergencia) y acústicas (como los sensores de ruptura). Todos estos productos cuentan con una alta calidad de operación, sin embargo, existen factores externos que merman su funcionamiento.

Por lo tanto, examinar las características físicas del entorno como contaminación en el ambiente (polvo, humedad del ambiente etc.), estructura y materiales usados en la construcción del edificio, etc. fueron de suma importancia ya que determinaron las condiciones eléctricas y el tipo de cableado necesarias para que el hardware operara con la mayor calidad posible.

Existen dos tipos de procedimientos para una instalación adecuada de sistemas con este tipo de tecnologías: por una lado las instalaciones visibles que requiere de ranuras sujetas a paredes y pisos para dirigir el cableado a las terminales eléctricas; por otra parte las ocultas donde los dispositivos son instalados sobre la losa con una placa protectora aislante.

Después de una exploración detallada del edificio que albergaría el sistema, nuestros compañeros determinaron que, por una parte. el inmueble no contaba con tuberías ni canalizaciones adecuadas para la instalación de los componentes y cableado del sistema. Por otra parte, al ser un área de laboratorios las condiciones ambientales eran húmedas, y oxidantes.

Aunado a estas condiciones, los materiales utilizados para la construcción del edificio no favorecían el aislamiento total de las canalizaciones por lo que se busco una alternativa que permitiera proteger el cableado de la mejor manera posible. De esta manera se optó por utilizar tubería conduit[1] en instalación visible.

Esta instalación incluye dos tipos de canalizaciones de acuerdo a los requerimientos del sistema de seguridad:

- Una canalización para la alimentación eléctrica de las antenas.
- Una canalización para la transferencia de datos.

Una vez determinado el tipo de instalación que más se adaptaba a las características del edificio, fue necesario establecer las características físicas que

[1] La tubería conduit es utilizada para la protección del cableado de líneas eléctricas, redes telefónicas y fibra óptica. Entre sus principales características son: resistencia al ataque de productos y sustancias químicas y corrosivas, bajo costo, facilidad de instalación y duración (inclusive en suelos agresivos).

deberían tener las canalizaciones que serían montadas; con el objetivo de dar el máximo soporte a las necesidades del proyecto.

Para ello nuestros compañeros hicieron la siguiente evaluación para cada unos de los elementos:

- Tipo de aislamiento y el calibre del conductor eléctrico a usar en la instalación.
- Diámetros de la tubería para la alimentación eléctrica.
- Capacidad del elemento termomagnético para proteger el sistema contra sobrecargas y cortos circuitos.

5.2.2 Costos de inversión y mantenimiento del sistema

En cualquier proyecto a desarrollar calcular todos los bienes y servicios requeridos es una parte fundamental en la cual se debe poner especial atención. Se debe considerar que los gastos no sólo involucran la adquisición de las herramientas necesarias para desarrollar el proyecto y el capital humano; sino que debe prever los gastos de instalación, operación y mantenimiento del sistema con el objetivo de obtener los mayores beneficios a un costo razonable.

En el caso particular del sistema de seguridad al estar inmerso en tecnología de punta, se debe considerar que el equipo cuente con la mejor calidad, eficiencia y durabilidad que garantice al usuario una completa restitución de su inversión.

5.2.3 El elemento humano

El objetivo principal del sistema de seguridad es proporcionar al usuario un sistema que permita incrementar la seguridad en el uso de sus instalaciones al proteger a sus miembros así como salvaguardar sus bienes; es un beneficio adicional que en ningún momento debe interrumpir o entorpecer las actividades cotidianas del usuario.

Por esta razón nuestros compañeros realizaron un estudio completo de las instalaciones para determinar la distribución del equipo, de manera que ningún elemento de la instalación estorbara el espacio libre para operarios y permitiera la libre circulación para el personal.

5.3 Instalación de los componentes

Una vez realizadas las consideraciones pertinentes se realizó la instalación física de los elementos, los cuales fueron montados en cinco etapas:

Primer etapa: Instalación de la tubería, cableado.

- Segunda etapa: Instalación de puertas, lectores de alta frecuencia y antenas.
- Tercer etapa: Instalación de los registros y transponders en los equipos
- Cuarta etapa: Instalación de sensores y actuadores

5.3.1 Primer etapa: Instalación de las tuberías y el cableado

La instalación de tuberías fueron realizadas por un proveedor de la UNAM, sin embargo la supervisión, cableado y remate de cada uno de los componentes fueron realizados por nuestros compañeros de proyecto, quienes se encontraron ante el arduo trabajo de coordinar y vigilar que cada uno de los elementos fueran colocados de acuerdo al diseño de instalación establecido por ellos.

5.3.2 Segunda etapa: Instalación de puertas, lectores de alta frecuencia TAG y antenas

De manera casi simultánea se realizó la colocación de las puertas por un grupo de carpinteros; con lo que se incrementó la responsabilidad de nuestros compañeros en vigilar que el proceso de instalación se efectuara adecuadamente, ya que estas puertas albergarían los sensores magnéticos, la chapa magnética, el módulo Receptor/Transmisor del interfón y los dos dispositivos más importantes: la antena para protección de equipo y el lector TAG para credenciales de usuarios (Ver figura 5.2).

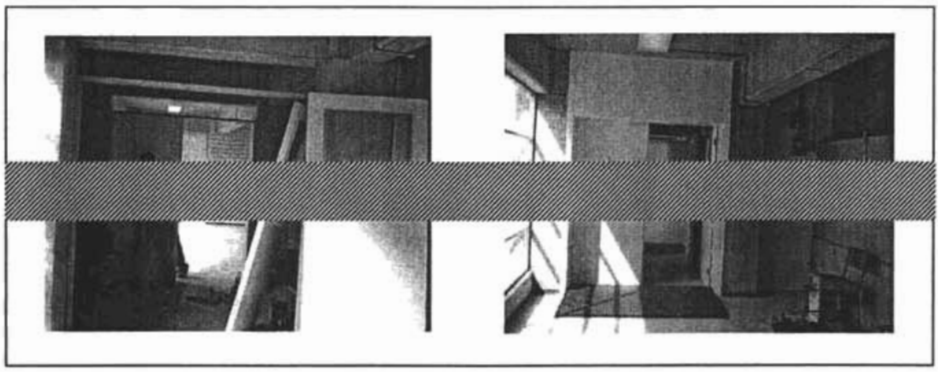


Figura 5.2 Instalación y terminado de las puertas de acceso en la planta alta

Antes de finalizar la colocación de las puertas se instalaron todos los dispositivos electrónicos que se encontrarían protegidos por estas. Las antenas para protección de equipo fueron colocadas estratégicamente en cada área y posteriormente configuradas para obtener su máximo rendimiento.

Los Lectores TAG destinados a la identificación de usuarios así como los módulos de Recepción/Transmisión de los interfones fueron instalados en la parte externa de las puertas a una altura de 1.20 m con respecto al nivel del piso para facilitar al usuario la interacción de su credencial con el módulo lector y con los interfones.

En la figura 5.3 se puede observar el Lector y al Receptor-Transmisor del Interfón.

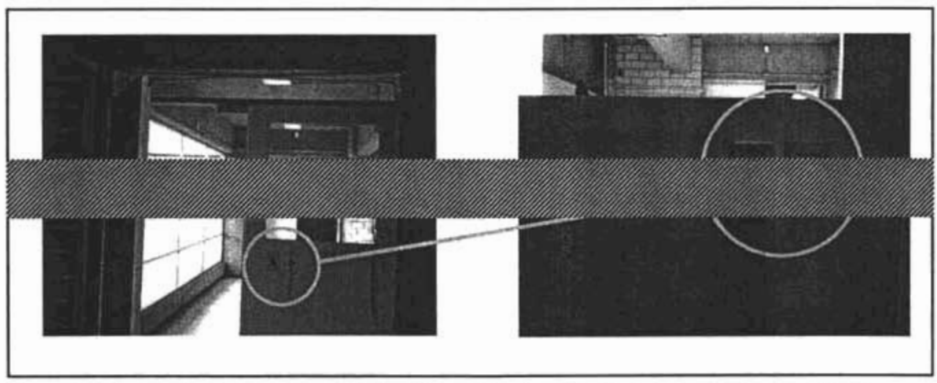


Figura 5.3 Receptor/Transmisor del interfón y el Lector TAG instalados en la puerta de acceso

5.3.3 Tercer etapa: Instalación de los registros, módulos de baja frecuencia (serie 2000) y los chips de identificación en los equipos (transponders)

Los registros, son gabinetes metálicos donde están colocados los módulos que habrán controlar las cuatro zonas del edificio. Son dos los tipos de registros que se colocaron, el registro series 2000 y el registro TAG, de este ultimo tenemos uno por zona controlada. Junto a cada registro TAG hay otro al que hemos llamado respaldo TAG, que contienen una fuente de alimentación, junto con un respaldo de baterías para alimentar la cerradura magnética y la alarma general
(Ver figura 5.4).

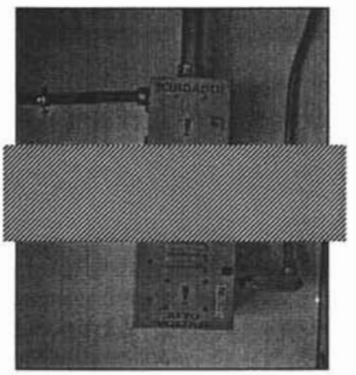


Figura 5.4 Registro y respaldo TAG.

El Registro Series2000 fue colocado a más de 2.50 m de altura del nivel del piso para asegurar que no estuviera al alcance de los usuarios con el equipo siguiente: Cuatro módulos Series2000, respaldo de energía con un No Break, fuente de voltaje de 12vcc. (Ver figura 5.5).

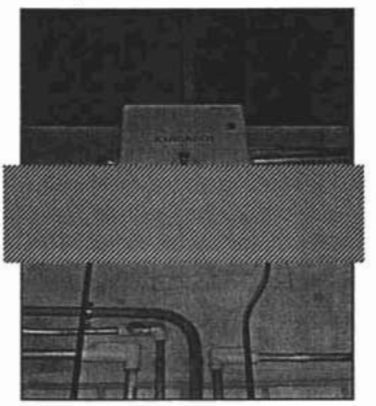


Figura 5.5 Registro series 2000

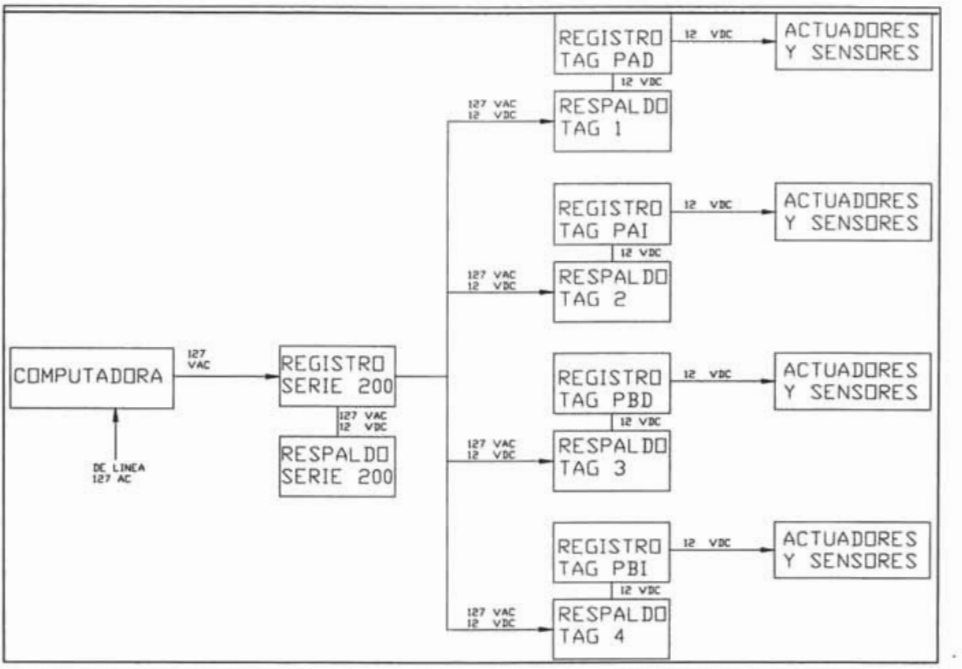


Figura 5.6 Registros TAG PC, de Izquierda a derecha y de arriba hacia abajo: planta baja Izquierda (PBI), planta baja derecha (PBD), planta alta izquierda (PAI), planta alta derecha (PAD).

Transponders. Como ya habíamos mencionado en capítulos anteriores se usaron dos sistemas de lectores, con dos frecuencias diferentes, el TAG es de alta frecuencia y el Series2000 de baja frecuencia. En la figura 4.10.1 se ve el Lector TAG y su transponder, en la figura 5.7 podemos ver el Series2000 y los diferentes tipos de transponders que usamos de este Lector en el proyecto.

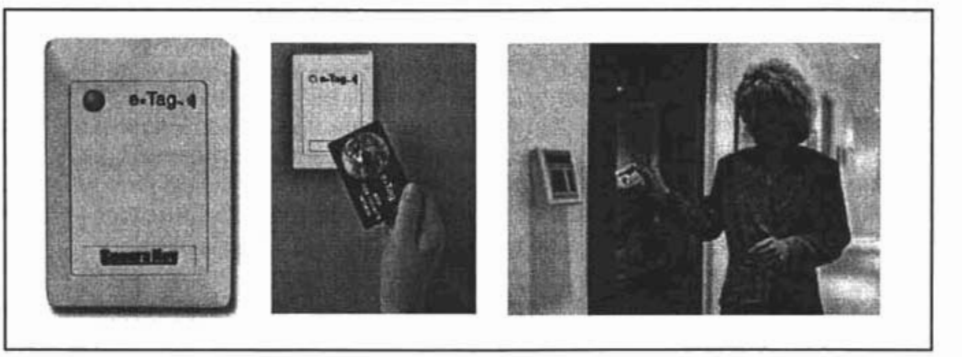


Figura 5.7 Lector TAG y su uso

Para los usuarios se uso el transponder de tipo credencial como el que se muestra en la figura 5.8, pero para los equipos se consideraron de diversos tipos. Cada equipo a proteger en el edificio tienen formas y materiales diferentes por lo que nuestros compañeros tuvieron que determinar cual transponder era el adecuado para cada equipo.

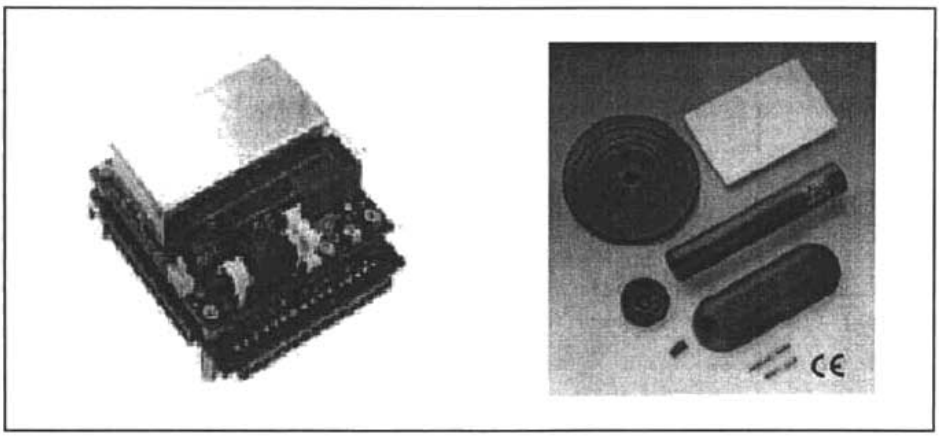


Figura 5.8 Lector Series2000 y los transponders usados en el Proyecto de Tarjetas Inteligentes.

A continuación presentamos con más detalle los tres tipos de Transponders del Series2000 que se instalaron en los equipos:

Small MOM (Small Mount – On – Metal Transponder), es usado para equipos que tengan un armazón de metal, por ejemplo el CPU de una computadora, este transponder responde mejor a la lectura cuando tiene una base metálica.

Large Disc, usado en equipos de laboratorio y aparatos electrónicos que no tengan armazón de metal. Este tipo se puede usar en monitores.

Cylindrical, es el transponder de mayor alcance, por lo que lo usamos en casi todos los equipos importantes, aunque fijarlo resultaba difícil, personal del C.D.M. nos recomendó pegamentos epóxicos para fijarlos al equipo.

En una junta realizada con personal del edificio en donde se iba a instalar el sistema y con los integrantes del proyecto se determinaron los equipos que se integrarían al sistema de protección. El número de equipos rebasaba el total de transponders que se tenían destinados para los equipos, pero se les dio prioridad a los más importantes, ya sea por su valor económico o académico.

La instalación para cada transponder y equipo fue diferente por lo que no se detallara la instalación de todos los transponders, pero comentaremos los más sobresalientes.

Instalación de los transponders en un sistema de computo:

Cada transponder instalado en los equipos tenía que estar en una posición estratégica, donde no pueda ser visto o de fácil acceso al usuario y que al mismo tiempo sea fácil la lectura para la antena del Lector Series2000. en la figura 5.9 se ve el tipo y la posición del transponder en cada uno de los componentes en un equipo de computo.

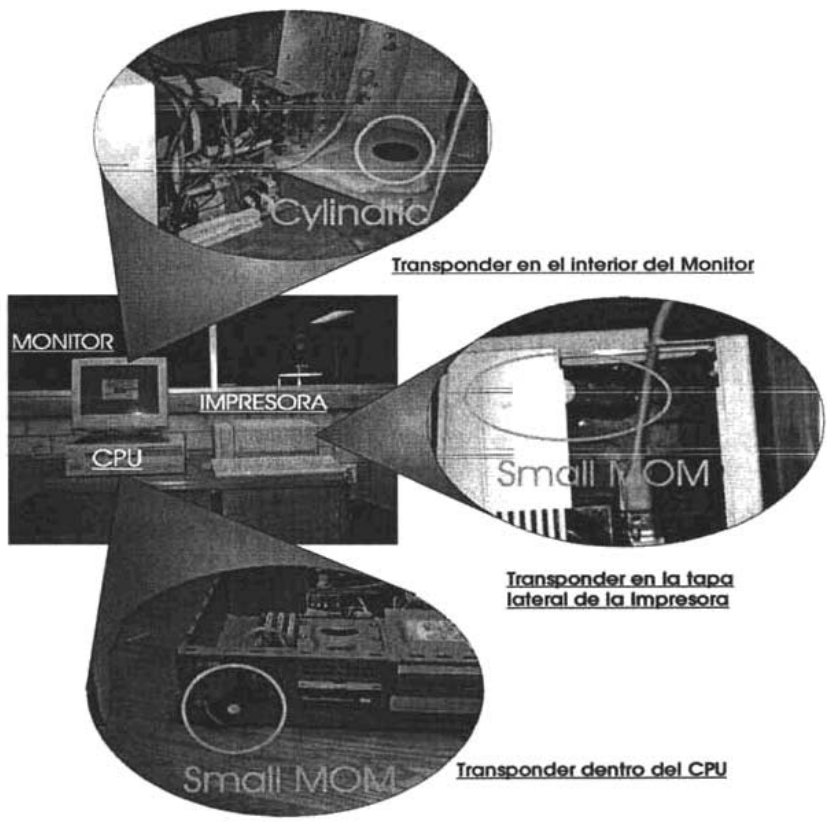


Figura 5.9 Posición de los transponders en un equipo de Cómputo.

Instalación de varios Transponders en un aparato:

Existen aparatos que son muy fáciles de mover y por lo tanto fáciles de extraer de los laboratorios, para estos equipos se tomo la decisión de ponerle dos identificadores, uno en cada extremo.

En la figura 5.10 se puede observar un ejemplo de este caso.

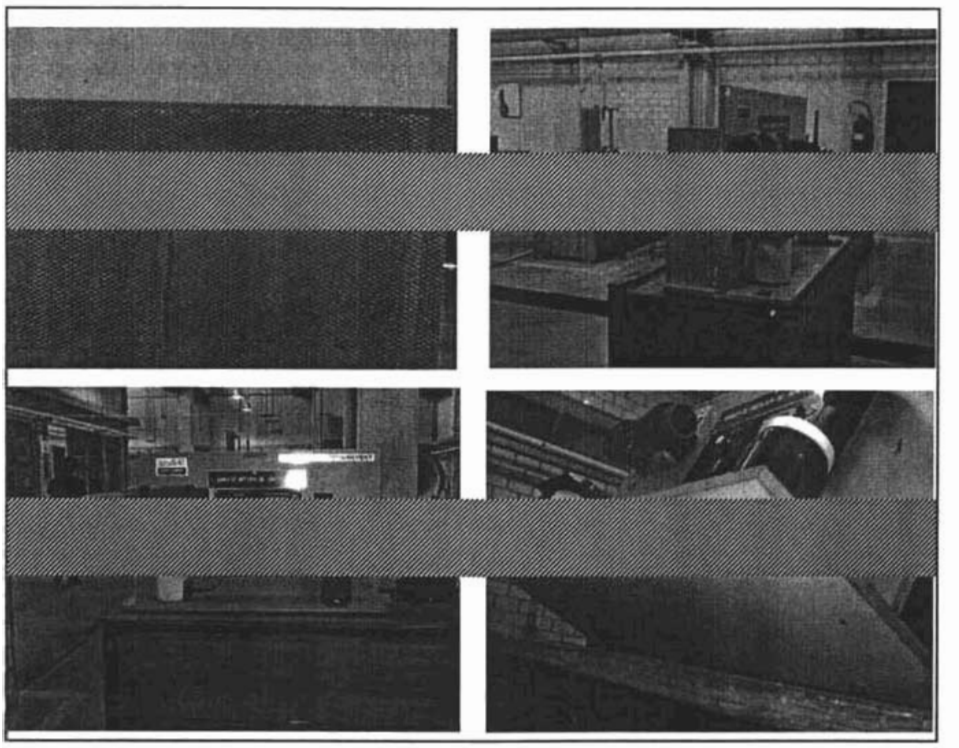


Figura 5.10 Dos transponders instalados. En las imágenes superiores se muestra la posición de un Small MOM y en la imagen inferior derecha se ve uno de Tipo Cylindric.

Instalación del transponder en un monitor con cubierta metálica:

Para los equipos que tienen armazón metálico el Transponder Small MOM es el ideal, el metal aumenta el área activa de lectura en las antenas. La figura 5.11 muestra un monitor con estas características y la posición del Transponder.

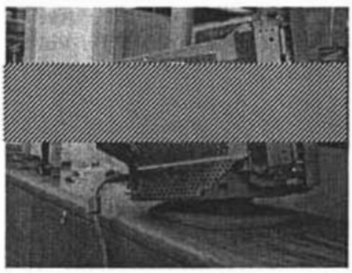


Figura 5.11 Transponder Small MOM en un Monitor.

Hubo casos en que los equipos están conformados por partes y se debían proteger cada una de ellas, en la figura 5.12 se puede ver un ejemplo:

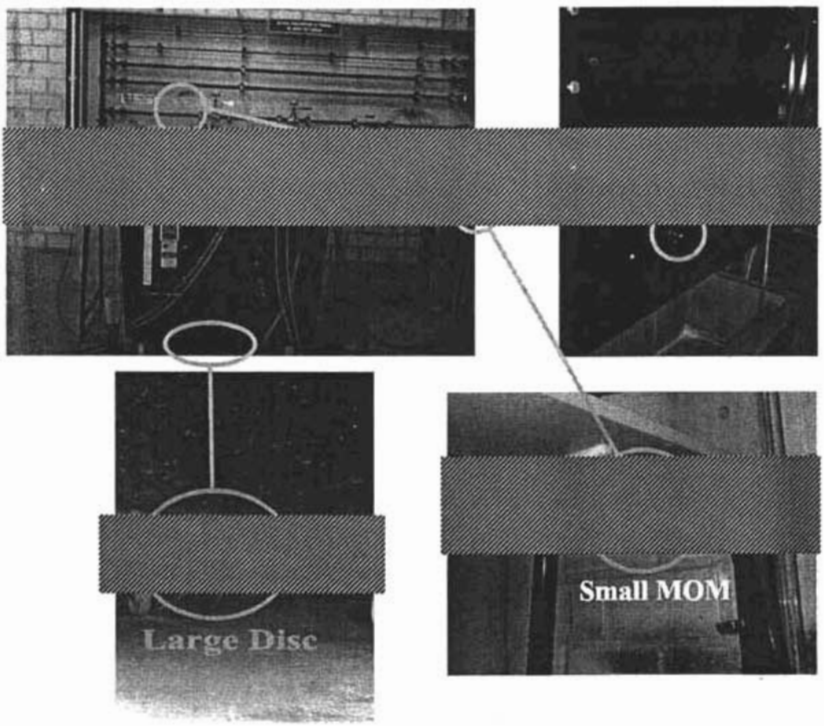


Figura 5.12 Tres transponders instalados en un equipo formado por tres partes, en este se uso además del Small MOM y Cylindrical el tipo Large Disc.

5.3.4 Cuarta etapa: Instalación de sensores y actuadores

Los sensores de movimiento se instalaron de tal manera que cubren toda el área por donde es posible que entre alguna persona, están instalándolos a una cierta altura y con un ángulo de inclinación, de tal forma que se activan antes de que la puerta se abra lo suficiente, para que una persona entre, es decir, el control maestro detecta el evento antes de que el intruso o usuario tenga la perspectiva del sensor.

Estos sensores tienen un horario definido de funcionamiento ya que durante el día las instalaciones son usadas constantemente, pero llega un horario en el que nadie debe ya entrar, en este lapso de tiempo es cuando funcionan los sensores de movimiento.

En la figura 5.13 se puede ver un sensor de este tipo ya instalado.

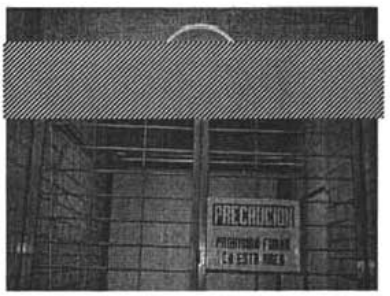


Figura 5.13 El círculo muestra la posición del sensor de movimiento

Los sensores de ruptura de cristal se instalaron en la parte alta de los ventanales de la planta alta de tal manera que protegen el ventanal y la ventana que se encuentra en las puertas de acceso, estos están activos las 24hrs del día.

Los sensores magnéticos están colocados en las puertas de acceso controlado por el sistema, su función es avisar cuando una puerta se ha abierto, al igual que los sensores de ruptura de cristal, estan activos las 24 horas del día.

Para finalizar esta breve reseña de la instalación del hardware se muestra el diagrama de bloques de la comunicación del sistema de acceso de personal y equipo.

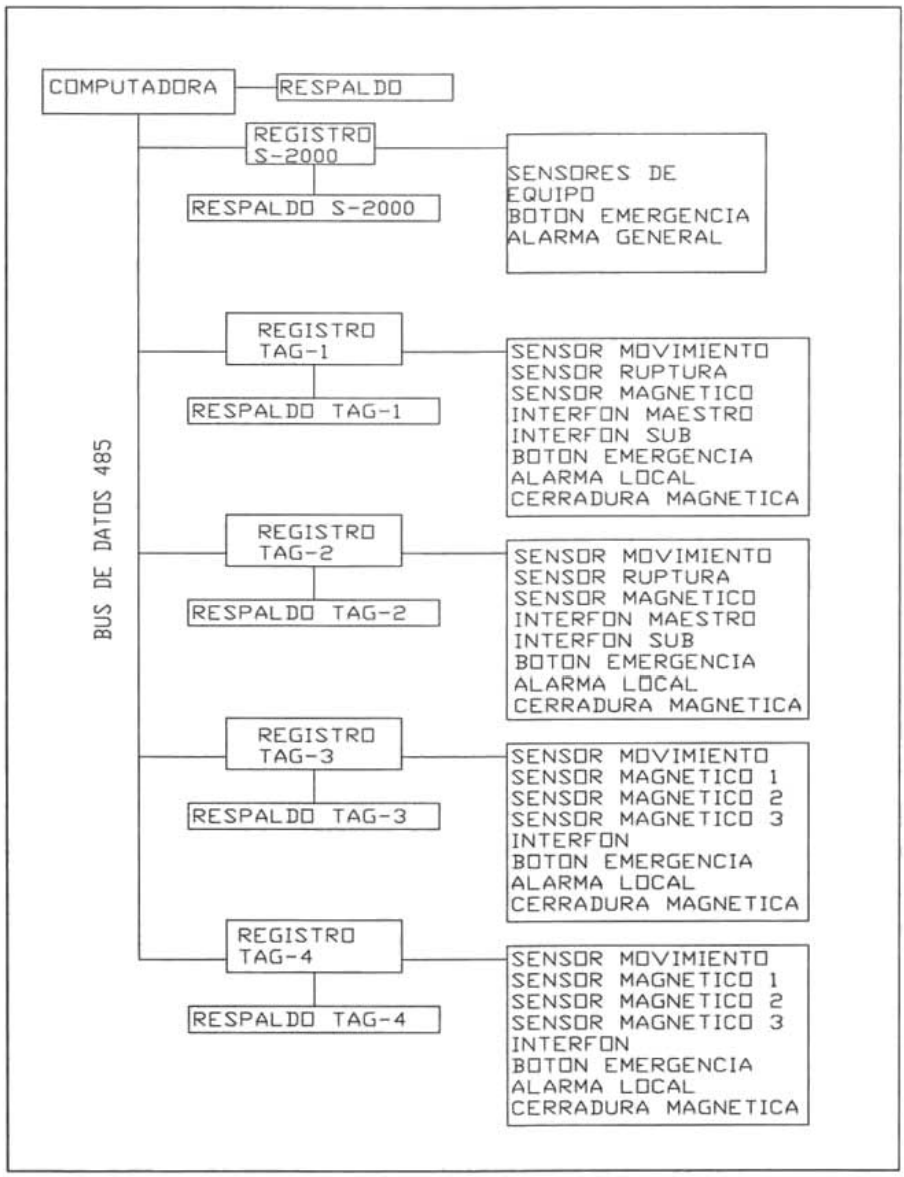


Figura 5.14 Diagrama de bloques de la comunicación entre los registros y la computadora.

5.4 Instalación de la versión final de la aplicación "SAPPE"

Una vez que los módulos de la aplicación estuvieron completos y ensamblados, el proceso siguiente, fue compilar todo el código para obtener un archivo final ejecutable.

Este proceso es realizado dentro del mismo entorno de Visual Basic donde al seleccionar la opción para crear un archivo ejecutable de la aplicación, el código escrito es traducido a código máquina y es analizado para comprobar que no existan incongruencias en la declaración de variables o funciones.

A partir del archivo ejecutable y mediante el "asistente para empaquetado y distribución" que proporciona Microsoft Visual Basic 6.0 creamos un instalador de la aplicación SAPPE V.0 El instalador es un paquete que contiene todos los archivos y librerías necesarios para que se ejecute el programa correctamente al ser trasladado a otras computadoras. De manera que al ejecutarlo en otro equipo automáticamente se iniciará la instalación del software como comúnmente se instala cualquier otro programa de cómputo tal como Windows, Office, etc.

Finalmente instalamos la aplicación en la computadora asignada para el sistema de seguridad.

Como esta aplicación es un sistema integral que interactúa con una Base de Datos y Hardware es necesario que antes de instalar SAPPE V.5 se cuente con el siguiente equipo de hardware y software correctamente configurado y funcionando:

- Manejador de Base de Datos Interbase 6.5 o superior. Sofware instalado en su versión completa de Servidor y con licencia para tres clientes simultáneos.

- ODBC de EasySoft para Interbase. Configurado de tal forma que el origen de datos sea la base de datos de SAPPE v.5 que se encuentra en la carpeta donde instalo el software.

- Módulo(s) de hardware del "Sistema Tarjetas Inteligentes" – TAG, Serie 2000, etc – conectados a la PC en cualquiera de sus puertos serie.

5.5 Pruebas

Una de las etapas más delicadas de la creación de software es el proceso de pruebas, ya que, además de consumir una gran cantidad de tiempo, exige un minucioso análisis que permita detectar la mayor cantidad de errores dentro de la aplicación.

No es conveniente que la etapa de pruebas se considere como el proceso final en la creación de un programa de aplicación, puesto que a medida que crezca el sistema se volverá más complejo detectar una falla en su estructura y más aún encontrar la línea de código exacta donde se está generando el problema. Por ello, consideramos que las pruebas deben ser programadas y realizadas antes, durante y después de comenzar el proyecto con el fin de asegurar que cada parte del sistema este funcionando de la mejor manera posible.

En la figura 5.15 Se muestra el proceso de pruebas realizado para validar y verificar la aplicación.

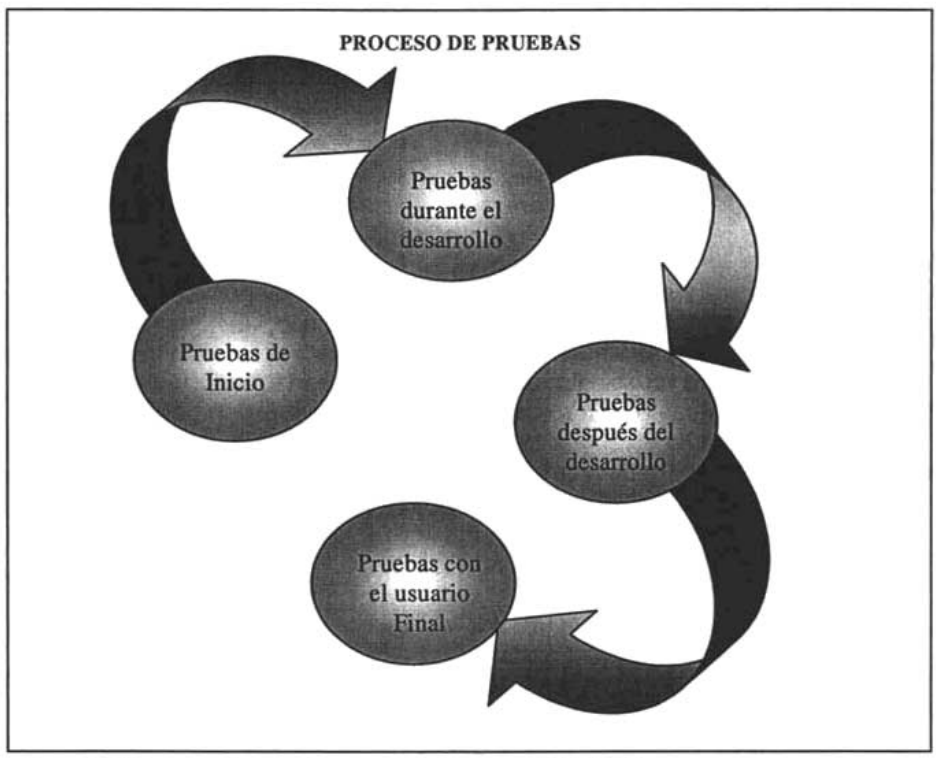


Figura 5.15 Proceso de pruebas para el programa SAPPE V.0

Con base en la figura 5.15 determinamos un plan de pruebas descrito a continuación:

Planificación de pruebas para el SAPPE

Bloques / Etapas	Comunicaciones	Bases de Datos	Seguridad	Interfaz
Pruebas de Inicio	◆			
Tiempo de Desarrollo	◆	◆	◆	◆
Después de la programación	◆	◆	◆	◆
Usuario Final				◆

Tabla 5.1 Planificación de pruebas del software.

A continuación presentaremos las pruebas realizadas para cada uno de los bloques así como el seguimiento que se le fue dando a través de las distintas etapas.

5.5.1 Pruebas de Inicio

En proyectos enfocados al desarrollo de nuevas tecnologías, las pruebas anticipadas proporcionan una herramienta de exploración para comprender de manera explícita la forma en que opera cada una de las partes del sistema y la forma en que habremos de interactuar con ellas para llegar a nuestros objetivos.

En nuestro caso particular realizar pruebas antes de comenzar a estructurar SAPPE V.0 fue fundamental, ya que este programa está orientado al control y operación de hardware de innovación tecnológica. Para poder diseñar e implementar la lógica operacional del sistema de seguridad, fue necesario comprender el funcionamiento de los dispositivos, su protocolo de comunicación y sobretodo la forma en que interactuaría con el software. Por ello consideramos de suma importancia, y como primer paso para la creación del sistema, realizar pruebas directamente con los dispositivos.

Para la realización de estas pruebas generamos un programa cuyo único objetivo fue mandar instrucciones de lectura a los dispositivos, cachar las cadenas de respuesta e interpretarlas. Estas pruebas permitieron comprobar:

- La forma en que debe ser enviada la instrucción para poder comunicarnos de manera adecuada con ellos.
- La estructura de la cadena de respuesta de los dispositivos, que posteriormente serían de gran utilidad para poder descomponer adecuadamente la cadena de acuerdo a nuestros intereses.
- Nos permitió establecer el protocolo de comunicación .
- Que funcionaba correctamente la comunicación entre los dispositivos y la computadora a través del puerto.

5.5.2 Pruebas durante el desarrollo

Las pruebas durante el desarrollo son pruebas informales que estuvimos realizando gran cantidad de veces con la finalidad de verificar que todo el código escrito hasta el momento se ejecutara correctamente.

En esta fase se probó cada uno de los módulos generados así como su integración con otros módulos. Para realizar pruebas de manera individual se simuló la entrada de datos correspondientes con los requerimientos de cada módulo.

A continuación haremos una breve explicación de las pruebas realizadas en cada uno de los módulos:

Comunicaciones

El módulo de comunicaciones implica todos los subprocesos relacionados con la transmisión, recepción y procesamiento de datos que circulan entre el hardware y la aplicación. Por lo que fue necesario realizar las pruebas directamente con cada tipo de dispositivo que iba a estar operando dentro del sistema.

Para ello requerimos que nuestros compañeros de electrónica nos proporcionaran un módulo de lectura de alta frecuencia, un módulo de lectura de baja frecuencia, sensores, y dispositivos que simularan la acción de los actuadores; así como tarjetas iguales a las que serían proporcionadas a los usuarios y chips como los que serían colocados para proteger el equipo. De esta manera pudimos recrear un sistema homólogo al que estaría operando la aplicación.

Bases de Datos

Una vez concluido el diseño conceptual y lógico de la Base de Datos se desarrollaron los módulos que interactuarían directamente con el motor de la base de Datos (Easysoft IB6 ODBC). Cada uno de estos módulos fue probado

manejando datos ficticios que simularían la información contenida en la Base de Datos real.
Se realizaron:

- Altas de usuarios y equipos
- Simulación de entradas y Salidas de Usuarios.
- Simulación de salidas de equipo
- Modificación de datos.
- Consulta de Información
- Generación de Reportes.

Para estas pruebas utilizamos un módulo de lectura conectado al puerto serie igual al que se utilizaría en las Instalaciones, credenciales como las que serían entregadas a los usuarios y chips como los que serían implantados en los equipos.

Interfaz

Dentro de la interfaz estuvimos verificando cada una de las rutas posibles generadas a partir de la selección de una opción, con el objetivo de comprobar que se ejecutaran todos los botones y menús y, se desplegara la información correctamente. Asimismo confirmamos que cada pantalla se desplegara de acuerdo a los privilegios del usuario.

A medida que íbamos avanzando en la programación de los módulos realizamos pruebas de integración entre ellos.

5.5.3 Pruebas después de la Programación

Después de haber revisado individualmente cada proceso de la aplicación así como la integración entre módulos, contamos con los elementos necesarios para realizar la instalación de la aplicación y las pruebas finales en el entorno real. Estas pruebas finales nos permitieron verificar que todos los procesos de la aplicación se ejecutaran correctamente en condiciones verdaderas y nos permitieron validar que la aplicación cumpliera con las especificaciones del cliente.

Durante el desarrollo se trataron de eliminar todas las posibles fallas en la ejecución de los procesos, sin embargo, al ser una aplicación dedicada a interactuar con elementos externos, se presentaron situaciones que alteraron el rendimiento de la aplicación.

Una de estas deficiencias fue el tiempo de verificación de cada uno de los dispositivos y por consiguiente la respuesta de acción de la aplicación. Al ser un sistema de seguridad, el tiempo de respuesta y acción, es un aspecto crítico. Durante el desarrollo, las pruebas se habían realizado con la computadora

conectada a muy corta distancia de los dispositivos, condición que cambio totalmente en las instalaciones. A pesar de haber considerado tiempos de respuesta teóricamente, de manera real, y debido a que las distancias se incrementaban para algunos de los dispositivos, los tiempos de respuesta se habían incrementado considerablemente por lo que se tuvo que buscar una solución efectiva que proporcionara el máximo rendimiento. Para ello tuvimos que ajustar el módulo de comunicaciones para que se adecuara a estas condiciones. La solución encontrada fue manejar tiempos de espera para cada área.

Otro problema que se presentó durante esta etapa de pruebas fue la forma en que configuramos el protocolo de comunicación para interactuar con el puerto serie, y más explícitamente con el control de flujo de la información, ya que originalmente determinamos que mediante señales XON-XOFF y RTS-CTS podría saber el puerto de comunicaciones en que momento enviar o recibir los datos, sin embargo, al transmitir la cadena existían valores que, codificados en ASCII, eran entendidos por el puerto como fin de transmisión lo que ocasionaba pérdida de datos y bloqueo del puerto. Para ello cambiamos esta configuración de manera que el puerto no utilizaría un control de flujo y la información la enviaría y recibiría sin tener que analizarla.

De manera general se realizaron pruebas de toda la aplicación tratando de cubrir todas sus vertientes. Para llevar un control de todas las revisiones hechas al programa definimos un plan que cubriera la mayor parte de los procesos de la aplicación. Esta exploración final la definimos en la siguiente tabla (Tabla 5.2) :

Bloque	Módulo	Operaciones	Resultado	Observaciones
Comunicaciones	Principal	• Monitorear los dispositivos • Controlar la lógica de los dispositivos • Restringir Horarios	Correcto	Se modificaron los tiempos de espera para recepción de datos de acuerdo al área del edificio.
	Puerto	• Configuración del Puerto de Comunicaciones	Correcto	Se cambió la configuración del Protocolo de Comunicación RS-232 a "Sin control de Flujo".
	Dispositivos	• Generación de Instrucciones • Agregar y eliminar dispositivos	Correcto	Se generaron matrices con las instrucciones a enviar en ASCCI, para disminuir los tiempos de procesamiento. Se configuraron las cuatros áreas del edificio conforme a los dispositivos instalados, y realizamos varias pruebas cambiando las restricciones de cada área para verificar que la aplicación reaccionara a los nuevos parámetros de forma congruente. Estuvimos generando situaciones de emergencia como activación de sensores de ruptura, sensores de movimiento, puertas abiertas en horarios no autorizados, y salidas de equipo no autorizadas para comprobar que el sistema reaccionara correctamente a cada estado de alerta.

Tabla 5.2 Resumen de las pruebas realizadas después de la programación.

Bloque	Módulo	Operaciones	Resultado	Observaciones
Bases de Datos	Altas	• Agregar usuarios • Agregar equipos	Correcto	Se dieron de alta varias credenciales de prueba con datos reales del personal y con diferentes restricciones para cada uno, posteriormente se estuvieron realizando accesos y salidas en todas las áreas mediante estas credenciales para probar que el sistema respetara correctamente las condiciones para cada usuario. Se dieron de alta algunos identificadores de equipo y se estuvieron probando salidas de equipos autorizados en distintos horarios, así como salidas de equipos no autorizados. Se agregaron opciones de configuración, para facilitar la captura de información del usuario. (Específicamente agregamos un cuadro de selección donde se despliegan todos los días de la semana para restringir el acceso por días, teniendo como parámetro inicial de lunes a viernes).
	Bajas	• Dar de baja Usuarios • Dar de baja Equipos	Correcto	Utilizando la misma información que generamos a partir de las pruebas de alta de usuarios, dimos de baja varias credenciales para comprobar que el usuario dado de baja perdiera todos los permisos de acceso, y únicamente se conservara su información.

Tabla 5.2 Resumen de las pruebas realizadas después de la programación. (Continuación)

	Cambios	• Modificar registros • Eliminar registros	Correcto	Estuvimos modificando información de los usuarios creados para realizar las pruebas, desde datos personales del usuario hasta sus restricciones de acceso. Para verificar que los cambios se ejecutaran correctamente realizamos accesos con las nuevas restricciones del usuario.
	Incidentes	• Registro de Incidentes de Usuarios • Registros de Incidentes de Equipos	Correcto	Se agregaron opciones de búsqueda, que facilitaran la consulta de incidentes.
	Restricciones	• Restricción de Acceso a Usuarios • Restricción de Salida de Equipo	Correcto	Se corrigieron botones del formulario que no estaban desplegando la información de manera correcta.
	Accesos y Salidas	• Registros de Accesos y Salidas de Usuarios • Registros de Salida de Equipos	Correcto	Se probaron todas las opciones posibles de restricción para el acceso de un usuario. Y todas las opciones posibles para salida de un equipo.
	Reportes	• Generación de Reportes de Usuarios, Equipos Incidentes	Correcto	Se generaron reportes de cada opción permitida por el sistema. Se hicieron algunas modificaciones en el diseño del reporte y desplegado de la información.
	Búsqueda	• Consulta y búsqueda de información en la BD	Correcto	Se realizaron varias búsquedas aleatorias.

Tabla 5.2 Resumen de las pruebas realizadas después de la programación. (Continuación)

Interfaz	Principal	• Acceso al módulo de comunicaciones. • Acceso al módulo de Bases de Datos. • Monitoreo de accesos y salida de personal. • Monitoreo de salida de equipo.	Correcto	Realizamos varios accesos y salidas de personal mediante credenciales dadas de alta para verificar la pantalla de monitoreo. Detectamos errores en el desplegado de accesos y salidas de personal, por lo que se modificó la función, así mismo agregamos un parámetro anteriormente no considerado (El área a la cual el usuario estaba accediendo).
	Interfaz Comunicaciones	• Botones y Pantallas para la administración manual de Dispositivos.	Correcto	Se comprobó que todas las opciones de configuración del módulo de comunicaciones se pudieran ejecutar.
	Interfaz Base de Datos	• Botones y Pantallas para las transacciones con la Base de Datos.	Correcto	Se comprobó que todos los botones desplegaran los datos, formularios y reportes de acuerdo a su propósito.

Tabla 5.2 Resumen de las pruebas realizadas después de la programación. (Continuación)

5.5.4 Pruebas con el usuario

Las pruebas que realiza el usuario son sin duda el parámetro más importante para definir que la aplicación es funcional y operativamente adecuada, ya que el usuario determinara si la aplicación cumple o no con los requerimientos establecidos y tienen la posibilidad de detectar errores que, nosotros como desarrolladores de la aplicación, difícilmente podríamos detectar.

Haciendo énfasis a este punto es muy frecuente que después de haber desarrollado una aplicación, como programadores ejecutemos de manera sistemática cada parte del programa limitando las posibilidades de exploración del sistema. A diferencia de nosotros el usuario, que no conoce el sistema, desarrollará su propio método de exploración y conocimiento del sistema por lo que puede detectar incongruencias o errores que nosotros pasamos inadvertidos.

Durante esta fase de prueba se designó un grupo de usuarios responsables de la administración del sistema , los cuales previamente fueron capacitados para el uso de la aplicación y manejo del hardware. Estuvimos al tanto de todos los detalles y sucesos originados durante este periodo, y mantuvimos una observación periódica de todos los elementos del sistema. Las observaciones de los usuarios durante esta etapa nos fueron de gran utilidad para el mejoramiento de la aplicación ya que sus nos permitieron el refinamiento de los procesos que involucran la interacción con el usuario.

5.6 Generación de manuales y capacitación de los usuarios

Una vez que estuvimos convencidos de que el sistema de seguridad estaba cumpliendo con los requerimientos especificados por el usuario y que la aplicación respondía plenamente a sus necesidades, tuvimos la pauta para continuar con el proceso de instalación y terminación del proyecto.

Existen dos aspectos importantes que considerar en la instalación de este sistema con respecto al personal de la organización, por una parte al ser un producto de innovación tecnológica los usuarios cuentan con muy poco o nulo conocimiento acerca de su operatividad, y por otra parte este sistema implica algunos cambios en los hábitos actuales del personal el cual tendrá que adaptarse a nuevos lineamientos de seguridad.

Por lo tanto es indispensable que proporcionemos al personal las herramientas necesarias para que haga un uso correcto del sistema y se adapte de manera sencilla a las nuevas políticas establecidas.

Para ello elaboramos un completo manual de operación por medio del cuál ofrecer al usuario un elemento de guía para usar cada parte de la aplicación de manera correcta. El manual consta de varios capítulos donde se describe de manera minuciosa cada uno de los formularios, procesos y eventos que forman el software del sistema; así mismo cuenta con capítulo dedicados a la descripción del hardware los cuales fueron elaborados por nuestros compañeros de proyecto.

Posterior al manual técnico, elaboramos un curso de capacitación que se impartió a un grupo de usuarios designados por el jefe de la organización, los cuales van a fungir como administradores del sistema. Este curso estuvo formado por dos partes:

- Una presentación impartida por el grupo de trabajo del proyecto, donde definimos desde las características globales del sistema hasta las características operativas y funcionales del hardware y el software.

- Una demostración del funcionamiento del sistema dentro de las instalaciones, donde por medio de credenciales y equipos de prueba, mostramos al personal la manera en que opera el sistema, el proceso de registro y administración de la información en la computadora, y el manejo de la aplicación para controlar los dispositivos, salidas de equipo y accesos de su personal.

Adicionalmente se elaboraron señalamientos de operación para el personal del edificio, por medio de las cuales se describe de manera ilustrativa el uso de los dispositivos. De esta forma los usuarios cuentan con instructivos resumidos en dispositivos de uso general como son los interfones y los dispositivos de control de acceso de personal.

5.5 Entrega del sistema de seguridad al usuario

Para culminar la instalación del proyecto se realizó el registro de la información concerniente al personal de la organización y el equipo a proteger en la Base de Datos. Para ello elaboramos formatos con los campos necesarios para llenar la Base de Datos del sistema de seguridad.

Los formularios concernientes al personal fueron entregados al jefe del edificio con el objetivo de que nos proporcionara la información personalizada de cada uno de los usuarios. Posteriormente se asignó una tarjeta de identificación a cada usuario y se generó su registro en la Base de Datos.

Cada una de las credenciales fue personalizada por el Departamento de Diseño del CDM. La credencial está formada por el nombre del usuario, actividad que desempeña, departamento al que pertenece y una fotografía que garantiza plenamente la identidad del usuario.

Por otra parte, la información de los equipos fue capturada de forma individual en la Base de Datos conforme se registraba, por medio de un aparato lector, el identificador del chip implantado en él; asegurando de esta manera la integridad de los datos.

Una vez capturada la información necesaria para comenzar a operar el sistema de seguridad se hizo entrega del sistema de seguridad al jefe del área, teniendo el sistema las siguientes características:

- Control de acceso de 4 áreas para personal y|o estudiantes.
- Control de equipo de 2 laboratorios.
- Control de equipo de cómputo para 2 áreas.

El sistema incluye:

100 Transponders (sensores) para equipo de cómputo y de laboratorio.
100 Credenciales personalizadas para el personal del edificio.
Sensores de Movimiento, Sensores de Ruptura de Cristal,
Sensores Magnéticos, Interpones, Botones de emergencia.
Dispositivos de acción como alarmas y cerraduras magnéticas.
Computadora personal.
Diseño de la credencial.
Software de validación de ingreso por base de datos.
Respaldo de baterías.
Cerraduras magnéticas para puertas.

5.6 Mantenimiento y mejoras al sistema

No existe software completamente libre de errores e imperfecciones. Por ello es necesario hacer revisiones periódicas que permitan detectar nuevas fallas, mejorar los procesos de la aplicación o bien incrementar su potencial.

Cuando un software no está desarrollado bajo un diseño bien estructurado los costos de mantenimiento pueden ser muy elevados para la empresa, inclusive aún más que el desarrollo de la misma aplicación, ya que muchas veces se requiere rehacer la aplicación para adaptarla a nuevas condiciones de operación.

Cuando diseñamos y desarrollamos el sistema SAPPE V.0 estábamos concientes de que este sistema estaba orientado al manejo de nueva tecnología y por lo tanto debía ser lo suficientemente robusto para adaptarse al continuo avance tecnológico. Por lo que asumimos la responsabilidad de hacer una aplicación que cubriera todos los requerimientos del usuario y al mismo tiempo tuviera la capacidad de expansión y adaptación a nuevas herramientas tecnológicas.

Bajo esta premisa diseñamos y desarrollamos la aplicación, como mencionamos en capítulos anteriores, con una estructura modular; que nos permitirá hacer cambios (en caso de requerirlos) sólo en los procesos específicos, sin que se vean alterados los demás módulos. Así mismo la Base de Datos por sus cualidades nos permitirá ofrecer un soporte continuo al crecimiento y protección de la información.

Los cambios que habrán de realizarse al sistema en un futuro, no sólo prevén el entorno tecnológico, sino las posibles necesidades que vaya generando el usuario conforme se introduzca en el manejo de la aplicación. Indudablemente que al tener nuevas necesidades se generarán requisitos que la aplicación deberá ir cubriendo.

Con respecto a este punto, después de haber realizado una junta con el personal del edificio donde fue implantado el sistema, tomamos sus impresiones con el objetivo de afinar algunos procesos y otorgar nuevas funciones al programa que facilitaran al usuario su operación.

De acuerdo con estas consideraciones establecimos un programa de mantenimiento que garantíce al usuario una herramienta constantemente funcional (Ver Figura 5.16)

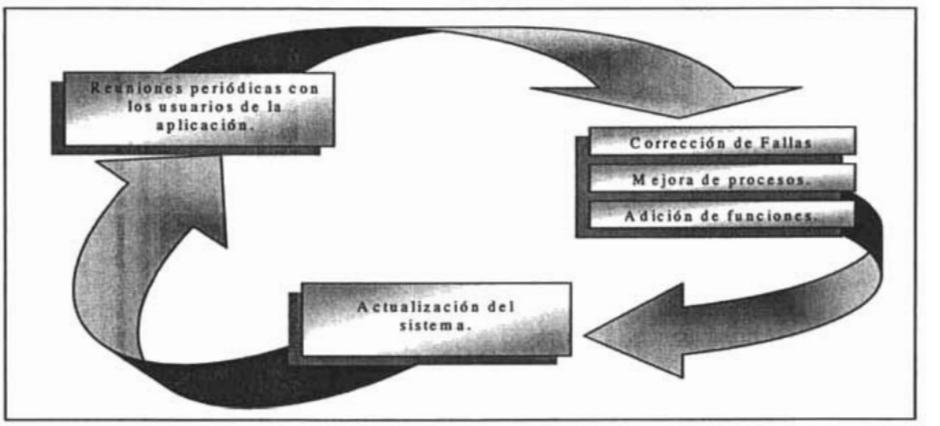


Figura 5.16 Proceso de mantenimiento

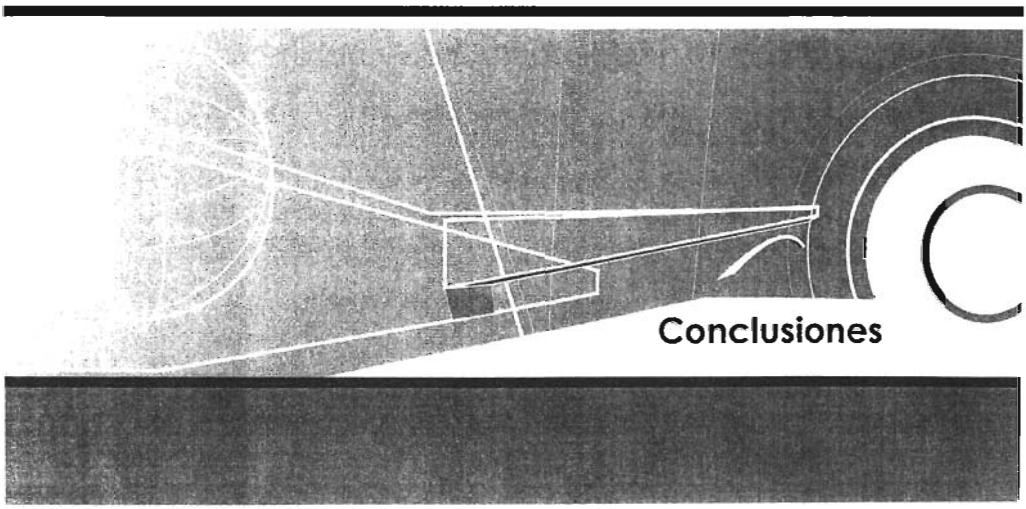
5.7 Notas a considerar para nuevos desarrollos

Aunque este proyecto llegó a buen termino, consideramos que existen algunas cuestiones que se pueden tomar como experiencia para futuros desarrollos y que causarán un impacto positivo para obtener aún mejores resultados. Por eso las mencionamos a continuación.

El Sistema funciona exactamente como esperamos que lo hiciera, no permite accesos en días y horas no autorizados, al detectar ruptura de cristales o activarse los sensores de movimiento activa alarmas, genera reportes, etc. Pero todo lo anterior no es suficiente sino existe una buena coordinación y compromiso con el personal de vigilancia, que a fin de cuentas son quienes actuarán en casos extremos. Si bien una alarma probablemente ahuyente a ladrones y el reporte impreso dará una idea de lo ocurrido, la verdadera acción queda en manos de las autoridades que deberán acudir al edificio y atrapar a los delincuentes.

Visual Basic fue una buena opción para nosotras como desarrolladoras, por ya contar con la herramienta y estar muy familiarizadas con el lenguaje. Sin embargo hubo algunas funciones que por las limitaciones del lenguaje no pudimos implementar y tomó mucho más tiempo buscar caminos alternos. Con otro lenguaje hubiera resultado sencillo. En específico necesitabamos hacer uso de hilos concurrentes para optimizar los tiempos de comunicación con los dispositivos pero este tipo de procesos en paralelo únicamente los soporta de manera nativa Java.

Otro buen motivo para mudar futuros desarrollos a dicho lenguaje, es que en determinado momento si se llega a contar con Sistemas similares en varios edificios. Será necesario intercambiar información a distancia y esto es también más sencillo haciendo uso de JDBC que permite enviar y extraer datos de manera remota y con un buen grado de seguridad.



Conclusiones

Conclusiones

Sin duda el trabajo en este proyecto ha sido arduo pero satisfactorio. A lo largo del proyecto hemos podido aplicar muchos de los conocimientos obtenidos durante la carrera en una situación práctica y además tuvimos la oportunidad de trabajar en equipo con personas de diversas áreas.

Apenas comenzabamos a bosquejar el proyecto cuando ocurrieron algunos robos en la Facultad que evidenciaron aún más la necesidad de contar con alternativas de seguridad eficaces. En ese sentido nuestro sistema ha demostrado cumplir con su cometido evitando el robo de bienes y proporcionando zonas seguras al personal. En el tiempo que lleva instalado incluso ya hemos tenido algunos casos de éxito donde se ha probado su utilidad, al evitar el acceso en horarios y zonas no permitidos con la activación de alarmas.

Por otra parte, el sistema ha sentado las bases e impulsado nuevos desarrollos orientados a la seguridad. De hecho, se han propuesto y aceptado ya, desarrollos similares para otras instalaciones en la Facultad. Y en lo que respecta a la tecnología empleada "la radiofrecuencia" consideramos que fue una excelente opción ya que esta en constante perfeccionamiento y cada día se encuentran dispositivos con mayor alcance y menor costo.

El software desarrollado cumplió completamente sus objetivos:

- Es capaz de controlar de manera eficiente y en tiempo real todos los dispositivos instalados,

- Al mismo tiempo que pone en ejecución el plan de seguridad de el edificio

- Y es una aplicación sencilla y fácil de emplear y por su diseño modular se puede escalar y/o adaptar a otras instalaciones.

En cuanto a la plataforma de desarrollo elegida obtuvimos los resultados esperados. El hecho de ser la más popular y la mejor manejada entre los usuarios, facilitó el aprendizaje y aceptación del software. Con esto nuestra aplicación es aún más sencilla y segura.

Las herramientas de desarrollo seleccionadas por ser familiares para nosotros, hicieron un poco más sencillo el desarrollo. Además que los productos elegidos son de amplia disponibilidad, con buena integración y amplio soporte técnico, con precios aceptables en especial en sus versiones acádemicas , que ayudaron disminuir los costos del proyecto.

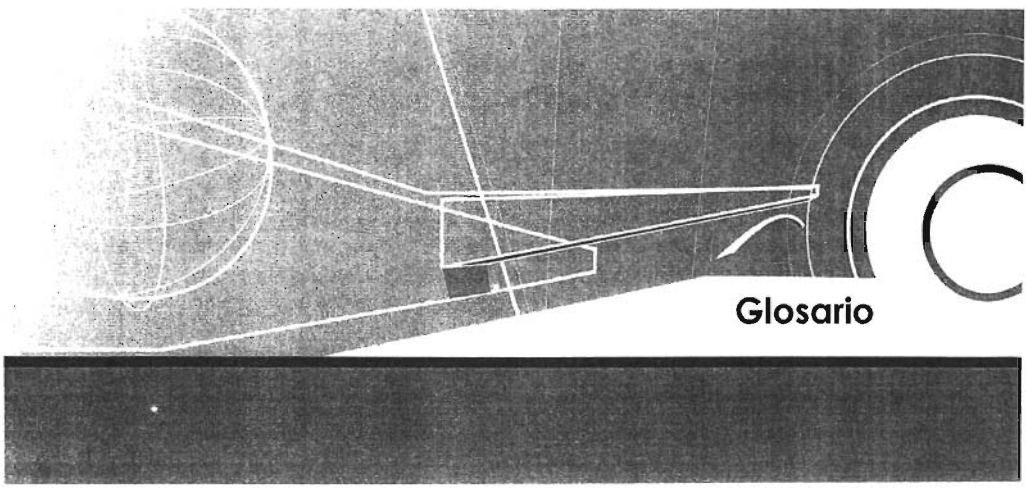
Así en una evaluación final, podemos decir que este trabajo satisfizo por completo las expectativas de todos los involucrados en el proyecto y nuestro

principal logro es ver el sistema funcionando, ser útil y cubrir las necesidades planteadas en un principio por los usuarios.
Particularmente logramos:

- Proporcionar al personal de la institución mayor seguridad, al garantizar que únicamente las personas autorizadas al área tendrán acceso.
- Garantizar la protección de equipo de las instalaciones.
- Un sistema autónomo que apoye en las tareas de vigilancia de instalaciones de la UNAM.
- Un software que responda a las necesidades planteadas por los usuarios
- Registro automatizado de personal.
- Registro automatizado de los eventos anómalos que se presentan durante el día.
- Sentar las bases de un proyecto para instalar el sistema en otras áreas de la Facultad de Ingeniería.
- Registro de Autor.
- Un prototipo que establezca una plataforma tecnológica para impulsar futuros sistemas que permitan la protección y seguridad no sólo del patrimonio de la Facultad sino de la Universidad.

Además que a nivel personal-profesional consideramos que el proyecto también rindió algunos frutos, también logramos:

- Habilidad para resolver problemas específicos en forma práctica.
- Conocimiento de nuevas tecnologías tanto del área afín como en otras áreas.
- Habilidad para realizar investigaciones que sean productivas para la comprensión y resolución de problemas.
- Capacidad para la toma de decisiones, trabajo en equipo y trabajo bajo presión.
- Conocimiento de nuevas herramientas tecnológicas que serán de utilidad para el desarrollo de nuevas aplicaciones en otros sistemas.
- Mayor seguridad y experiencia para desenvolvernos en el ámbito profesional.
- Administración de proyectos.



C

Glosario

Glosario

Amplitud de onda

Altura máxima que alcanza una señal, analógica o digital, con respecto al eje del tiempo, la cual indica la medida o el valor de la intensidad de dicha señal.

Antena

Conductor, conjunto o sistema de conductores (hilos, varillas) o dispositivo de cualquier clase destinado a la irradiación o la captación de ondas radioeléctricas. La antena tiene la misión de acoplar el emisor o el receptor, según el caso, con el espacio o medio por el cual se propagan las ondas. Las dimensiones físicas de la antena deben ser grandes en relación con la longitud de las ondas. Las antenas constituidas por un hilo o conductor casi nunca son de menos de un cuarto de la longitud de onda, y pueden tener desde un medio hasta varias veces la longitud de onda.

Autenticación

El proceso de verificar la identidad de un usuario en un sistema de seguridad. Se utiliza también para verificar la identidad de un mensaje.

Barra de Herramientas

Lista de iconos que al dar clic sobre ellos ejecutan de manera instantánea acciones específicas del software en ejecución.

Biométrica

Ciencia que estudia las características biológicas del ser humano (el iris, la huella dactilar, la voz, etc...) para su aplicación a la seguridad informática como medio de identificación del usuario.

BIOS

Basic Input/Output System: Sistema básico de ingreso/salida de datos. Conjunto de procedimientos que controla el flujo de datos entre el sistema operativo y dispositivos periféricos tales como el disco duro, la tarjeta de video, el teclado, el mouse y la impresora. El BIOS suele localizarse en un chip ROM o en un chip de memoria flash que puede actualizarse de ser necesario.

Campo electromagnético

Región del espacio en que se manifiestan las fuerzas eléctricas y magnéticas de una señal; en particular, dícese del campo asociado a una radiación electromagnética, que se manifiesta como dos campos, uno eléctrico y otro magnético que avanzan en dirección de la propagación, manteniéndose perpendiculares entre sí.

Canal

Medio físico a través del cual viaja la información, asignada a una finalidad específica, de un punto a otro. Las características que debe tener un canal son de gran importancia para lograr una comunicación efectiva, ya que de ellas depende en gran medida la calidad de la señal recibida en el destino. Varios canales pueden compartir un trayecto común; por ejemplo en cada
canal puede determinarse una banda de frecuencias o un intervalo específico.

Chip

Forma genérica de llamar a cualquier circuito integrado y encapsulado.

Cifrado

Es un método de encriptación, que utiliza típicamente una clave predefinida y un algoritmo para transformar texto simple en texto cifrado.

Circuito Integrado

Es un dispositivo electrónico compuesto por un conjunto de componentes conectados permanentemente entre sí e incluidos en una placa de silicio de menos de 1 mm2, formando un conjunto en miniatura. En un circuito integrado, los componentes activos, diodos, transistores, etcétera, y los componentes pasivos, resistencias, condensadores, etcétera, están integrados dentro de un mismo bloque llamado sustrato.

Codificación

Método por el cual se establece un cierto código o lenguaje de comunicación para la transmisión de información, ejemplos de codificaciones son: el sistema Braile, la señalización por banderas.

Codificador

Dispositivo que convierte señales analógicas a códigos digitales; es decir, codifica las señales que entran a éste. Las señales van enrrutadas de acuerdo a una clave o código que se le asigna previamente a cada señal. Por ejemplo, la voz puede convertirse en señal digital mediante un micrófono conectado a un transductor de impulsos luminosos (rayo láser) para las grabaciones de discos compactos, los cuales regeneran el patrón de voltaje determinado por la intensidad y frecuencia del sonido emitido por el micrófono. El codificador utiliza el sistema de números binarios (0 y 1) para expresar toda la información sobre las frecuencias y los niveles de voltaje. Por ejemplo, una fotografía puede ser descrita por una larga serie de unos y ceros, codificados de manera que algunos den información sobre la ubicación de los puntos que componen la imagen, y otros determinen la brillantez y el color de tales puntos. Las computadoras usan exclusivamente mensajes codificados digitalmente.

Código
Sistema de reglas que definen una correspondencia entre dos vías de información y se representa por caracteres, símbolos o elementos de señal como en el caso de los dígitos binarios (0 y 1). El alfabeto es un ejemplo de código.

Código 39

Simbología que se desarrolló en el año 1974, porque algunas industrias necesitaban codificar el alfabeto así como también números en un código de barras,. Es un estándar no utilizado para la industria alimenticia. Generalmente se utiliza para identificar inventarios y para propósitos de seguimiento en las industrias, es decir esta simbología es actualmente la más usada para aplicaciones industriales y comerciales para uso interno ya que permite la codificación de caracteres numéricos, letras mayúsculas y algunos símbolos como -, ., $, /, +, % y "espacio". Se utilizan sólo dos grosores tanto para barras como para espacios.

Código de Barras

Es una disposición en paralelo de barras y espacios que contienen información codificada en las barras y espacios del símbolo.

Cuadro de Diálogo

Ventana que contiene texto y uno o más botones que permiten al usuario darle instrucciones a un programa en ejecución.

Decodificación

Acción contraria a la codificación, donde se restablece la señal previamente codificada a su forma original.

EEPROM

Electricaly erasable programable read olny memory. Tipo de EPROM que se borra electricamente.

Encriptación

Se refiere al proceso de convertir datos en texto cifrado para evitar que terceras personas lo puedan ver o acceder.

EPROM

Erasable programable read olny memory. Tipo de PROM que se borra mediante la exposición a rayos ultravioletas. Para esta operación dispone de una ventana de cuarzo transparente a los rayos ultravioleta y una vez borrados los datos se necesita disponer de un grabador especial para introducir nuevos datos.

Frecuencia

Número de ciclos completos por unidad de tiempo para una magnitud periódica, tal como la corriente alterna, las ondas acústicas u ondas de radio. Se considera como el número de repeticiones de un fenómeno determinado en un intervalo de tiempo específico.

GSM

Global System for Mobile Communications; Sistema Global para Comunicaciones Móviles. Originalmente desarrollado como estándar europeo para la telefonía móvil digital, GSM se ha convertido en el sistema móvil de uso más difundido en el mundo. Se usa en las frecuencias de 900 y 1800 MHz en Europa, Asia y Australia y en la frecuencia de 1900 MHz en Norteamérica y Latinoamérica.

Icono

Símbolo gráfico que representa una determinada acción a realizar por el usuario por ejemplo: ejecutar un programa o imprimir un texto, etc.

Longitud de onda

Distancia que existe entre dos puntos de igual fase pertenecientes a dos ciclos consecutivos; se puede medir de cresta a cresta o de valle a valle en ondas sucesivas.

Memoria

Se designa de este modo a un área de almacenamiento de una computadora que contiene datos e instrucciones.

Modulación

Proceso para transformar la información de su forma original a una forma adecuada para su transmisión. La modulación se realiza en un transmisor, en el circuito llamado modulador.

Las principales razones para modular una señal son:
· Facilita la propagación de la señal.
· Optimiza el ancho de banda.
· Evita interferencia entre canales.
· Protege a la señal de la degradación de ruido.
· Define la calidad de la información.

Onda

Perturbación física o mecánica (movimiento ondulatorio) en un medio elástico (como el aire). Es preciso reconocer que no todas las perturbaciones son necesariamente mecánicas; por ejemplo, las ondas de luz, las ondas de radio y de radiación térmica propagan su energía por medio de perturbaciones eléctricas y magnéticas.

Onda de radiofrecuencia

Frecuencia a la cual la radiación de energía electromagnética es útil para las comunicaciones, el rango comprendido es superior a las frecuencias acústicas, pero inferior a la de la luz y el calor.

Onda electromagnética

Onda que está constituida por campos eléctricos y magnéticos que se propagan a través del espacio en forma perpendicular. Los campos magnéticos y eléctricos que son producidos por una antena viajan grandes distancias y transportan energía, a esto se le denomina radiación.

Polarización

Acción y efecto de hacer que la forma en que se propaga una onda electromagnética varíe en cuanto a la dirección de los vectores eléctrico y magnético. El campo eléctrico determina la forma en que se propaga una onda electromagnética, ya sea vertical u horizontal.

PROM

Programmable Read-Only Memory: Memoria de Sólo Lectura Programable. Es un chip de memoria en el que los datos pueden escribirse sólo una vez. Una vez que un programa escribe datos en la PROM, éstos permanecen ahí indefinidamente, incluso si la computadora fuera apagada. La diferencia entre una PROM y una ROM (read-only memory) es que la PROM se fabrica como memoria en blanco, mientras que la ROM se programa durante el proceso de manufactura. Para escribir datos en un chip PROM es necesario un dispositivo especial llamado programador PROM.

RAM

Random Acces Memory: Memoria de acceso aleatorio. Memoria donde la computadora almacena datos que le permiten al procesador acceder rápidamente al sistema operativo, las aplicaciones y los datos en uso. Tiene estrecha relación con la velocidad de la computadora. Se mide en megabytes. Hay dos tipos de RAM: RAM dinámica (DRAM) y RAM estática (SRAM), siendo la dinámica la más utilizada. Estos dos tipos se distinguen por la tecnología que usan para almacenar datos. La DRAM necesita una carga contínua de electricidad (refresh) para mantener la información. La SRAM no necesita esto, lo que la hace más veloz; aunque es también más cara que la dinámica. Ambos tipos de RAM son volátiles, o sea que pierden sus contenidos cuando se apaga el equipo.

Reader

Lector, Dispositivo que contiene la electrónica digital que activa un transponder para responder y extrae y valida la información de la respuesta modulada RF del transponder. También puede pasar los datos a un proceso posterior controlado por un computador central. Cuando el equipo es capaz simplemente de capturar

los datos del transponder, se llama un lector. Cuando el equipo también pueden escribir datos en el transponders, se llama un interrogador.

ROM

Read Only Memory: Memoria de Sólo Lectura. Memoria incorporada que contiene datos que no pueden ser modificados. Permite a la computadora arrancar. A diferencia de la RAM, los datos de la memoria ROM no se pierden al apagar el equipo. La ROM almacena programas críticos como el que permite arrancar la computadora. También se usan en calculadoras y dispositivos periféricos como impresoras láser, en las que las fuentes se almacenan en ROMs.

Señal

Conjunto de ondas propagadas a lo largo de un canal de transmisión que sirven para actuar sobre un dispositivo receptor.

Símbolo

Un símbolo de código de barras es la visualización física, es la impresion de un código de barras.

Simbología

La "simbología" es considerada el lenguaje de la tecnología de código de barras. Una simbología es la forma en que se codifica la información en las barras y espacios del símbolo de código de barras. Cuando un código de barras es digitalizado, es la simbología la que permite que la información se lea de manera precisa. Y cuando un código de barras se imprime, la simbología permite a la impresora comprender la información que necesita ser turnada dentro de una etiqueta.

Simbología EAN

European Article Numbering es el sistema de codificación EAN es usado tanto en supermercados como en comercios. Es un estándar internacional, creado en Europa y de aceptación mundial. Identifica a los productos comerciales por intermedio del código de barras, indicando país-empresa-producto con una clave única internacional. Hoy en día es casi un requisito indispensable tanto para el mercado interno como internacional.

Simbología UPC

Universal Product Code es la simbología más utilizada en el comercio minorista de EEUU, pudiendo codificar solo números. El estándar UPC (denominado UPC-

A) es un número de 12 dígitos. El primero es llamado "número del sistema". La mayoría de los productos tienen un "1" o un "7" en esta posición. Esto indica que el producto tiene un tamaño y peso determinado, y no un peso variable. Los dígitos del segundo al sexto representan el número del fabricante. Esta clave de 5 dígitos (adicionalmente al "número del sistema") es única para cada fabricante, y la asigna un organismo rector evitando código duplicados. Los caracteres del séptimo al onceavo son un código que el fabricante asigna a cada uno de sus productos, denominado "número del producto". El doceavo carácter es el "dígito verificador", resultando de un algoritmo que involucra a los 11 números previos.

Sistema biométrico

Se entiende por sistema biométrico todo aquel que es automatizado, que realiza labores de reconocimiento mediante una característica personal que puede ser reconocida o verificada.

El uso de la biometría permite reconocer al usuario a partir de un rasgo físico o hábito concreto. Entre los rasgos físicos se incluye: Huellas dactilares, la retina, el iris del ojo, la geometría de la mano y la imagen del rostro. Entre los hábitos o características susceptibles de ser reconocidas cabe citar los patrones de voz, ritmos de pulsación y firmas.

Sistema de comunicación punto a punto

Método de comunicación que abarca a un solo emisor y a un solo receptor únicamente.

Sistema de comunicación punto-multipunto

Método de comunicación que abarca a un solo emisor y a dos o más receptores en una transmisión simultáneamente.

TAG

Término comunmente empleado para hacer referencia a un transponder.

Tarjeta Inteligente

Es un plástico del tamaño de una tarjeta de crédito, que se utiliza en diversas aplicaciones. Estas tarjetas contienen uno o más chips semiconductores de silicio. El chip puede tener dos funciones, ser un poderoso microprocesador o actuar como un chip de memoria. El chip de silicio tiene tres funciones principales:

a) almacenamiento de datos.

b) seguridad en la información.

c) procesamiento de datos.

La ISO ha definido a las tarjetas inteligentes formalmente con el estándar 7816.

Existen diferentes categorías de tarjetas inteligentes , las cuales son categorizadas por tecnología y por la capacidad. En la categoría de tecnología, existen dos tipos:

- Tarjeta inteligente de contacto, la cual contiene un chip en la superficie de la tarjeta en conformidad con el estándar de ISO 7816.
- Tarjeta inteligente sin contacto, las cuales realizan la conexión por medio de transmisiones de radio frecuencia.

Texto cifrado

Es el texto que ha sido encriptado con un algoritmo y clave de encriptación.

Tiris

Texas Instruments Radio Frequency System. Acrónimo del sistema de identificación por radiofrecuencia de Texas Instruments.

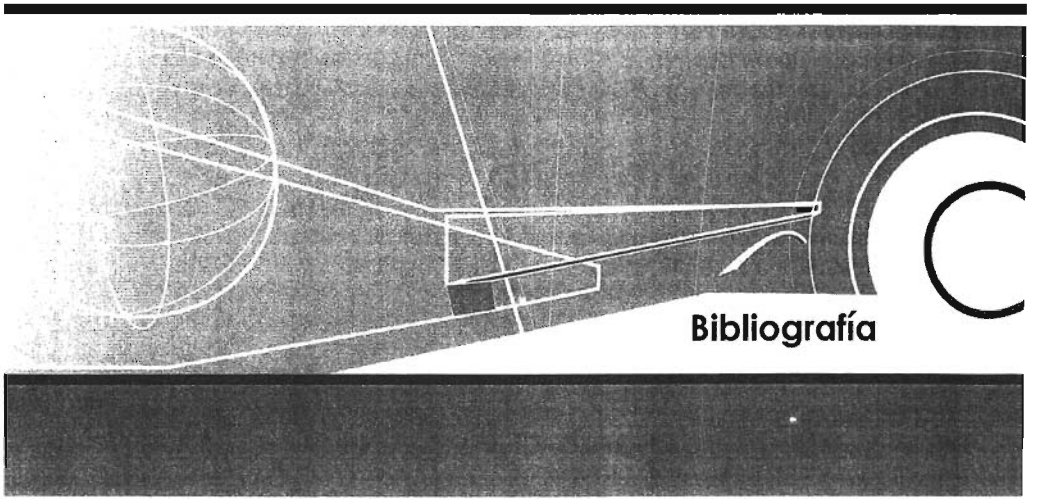
Tiris Bus Protocol

Es el protocolo que define el formato, contenido y significado de los mensajes que se intercambian entre los dispositivos lectores (readers) y el dispositivo maestro (master host). El protocolo esta diseñado para permitir la comunicación eficiente entre un único maestro y múltiples dispositivos esclavos con un mínimo de complejidad en el software.

Todas las comunicaciones son iniciadas por el dispositivo maestro mientras que los esclavos únicamente envían información únicamente a petición explícita del maestro.

Transponder

Transmisor/receptor electrónico que se adjunta al objeto a ser identificado y, cuando se reciben las señales apropiadas, transmite información a un lector en forma de señal de radio. A menudo llamados TAG (etiqueta).



C

Bibliografía

Bibliografía

Publicaciones Impresas

BARRANCO , Jesús. *Metodología del Análisis Estructurado de Sistemas.* 2ª ed. Madrid: Universidad Pontificia Comillas de Madrid, 2001. 320p. ISBN: 84-8468-043-6

CAPEL, Vivian. *Alarmas Contra Robos.* Yanque, Alejandro (trad.). Madrid: Parainfo, 1983. 193 p. ISBN: 84-283-1205-2

CEBALLOS, Francisco. *Visual Basic 6: curso de programación.* México: Alfaomega, 1999. 498 p. ISBN: 970-15-0447-X

GARCIA-PELAYO, Ramón. *Pequeño Larousse Ilustrado.* 19ª ed. México: Larousse, 1995. 1663 p. ISBN: 970-607-373-6

HANSEN, Gary; Hansen, James. *Diseño y Administración de Bases de Datos.* Katrib, Miguel (trad.); Dormido, Sebastián (Rev. Tec.); Otero, Andrés (ed.) 2ª ed. Madrid: Pearson Educación, 1997. XX p. ISBN:0-13-308800-6

KROENKE, David. Procesamiento de Bases de Datos. García, Ana Elizabeth (trad.); Esparza, Juan Raúl (Rev. Tec.). 8ª ed. México: Pearson Educación, 2003. 408 p. ISBN: 970-26-0325-0

MICROSOFT PRESS. *MS Visual Basic 6.0 Biblioteca de Referencia.* 2ª ed. México: McGraw-Hill, 2002. 3v. ISBN: 157-23-1864-3

TRAISTER, John. *Design and Application of Security/Fire-Alarm Systems.* New York: McGraw-Hill, 1981. 176 p. ISBN: 0-07-065114-0

Textos Electrónicos

ENCYCLOPEDIA BRITANNICA. *Security and Protection Systems* [en línea]. Encyclopedia Britannica Premium Service.[Consulta: Abril, 2004]. Disponible en Web: < http://www.britannica.com/eb/article?tocId=9066533>

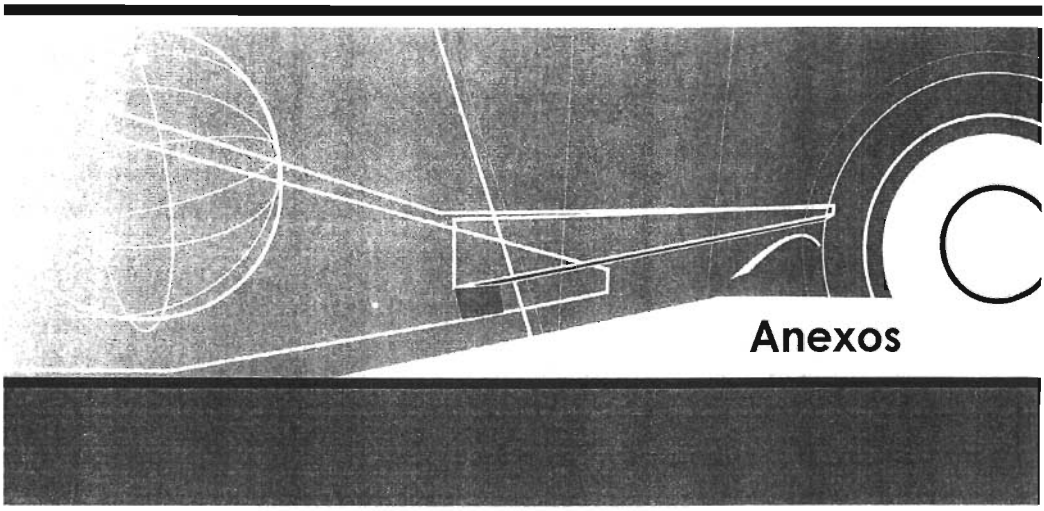
SECTRA-Sistemas Inteligentes de Transporte. *Glosario de Términos Relacionados con ITS [en línea].* Aristo Consultores. Santiago de Chile: Septiembre 2000. [Consulta: Septiembre, 2004]. Disponible en Web: http://www.sectra.cl/its/glosario/terminos.htm

EGOMEXICO-Expertos en RFID. *Glosario [en línea].* México: Agosto 2004 [Consulta: Septiembre, 2004]. Disponible en Web: http://www.egomexico.com/glosario.htm

YANINA, María. *Simbología en código de barras...[en línea].* Morea, Lucas. Argentina: Agosto 2004 [Consulta: Septiembre, 2004]. Disponible en Web: http://www.monografias.com/trabajos11/yantucod/yantucod.shtml#SIMBOL

AMIPCI. Glosario de Internet *[en línea].* México: Septiembre 2004 [Consulta: Septiembre, 2004]. Disponible en Web: http://www.amipci.org.mx/glosario.html

TEXAS INSTRUMENTS. *Series 2000 Reader System Tiris Bus Protocol (Reference Guide) [documento PDF, en línea]. Estados Unidos : Marzo 2000.* [Consulta: Enero, 2003]. Disponible en Web: http://www.ti.com/tiris/docs/manuals/refmanuals/s2000bus.pdf



Anexos

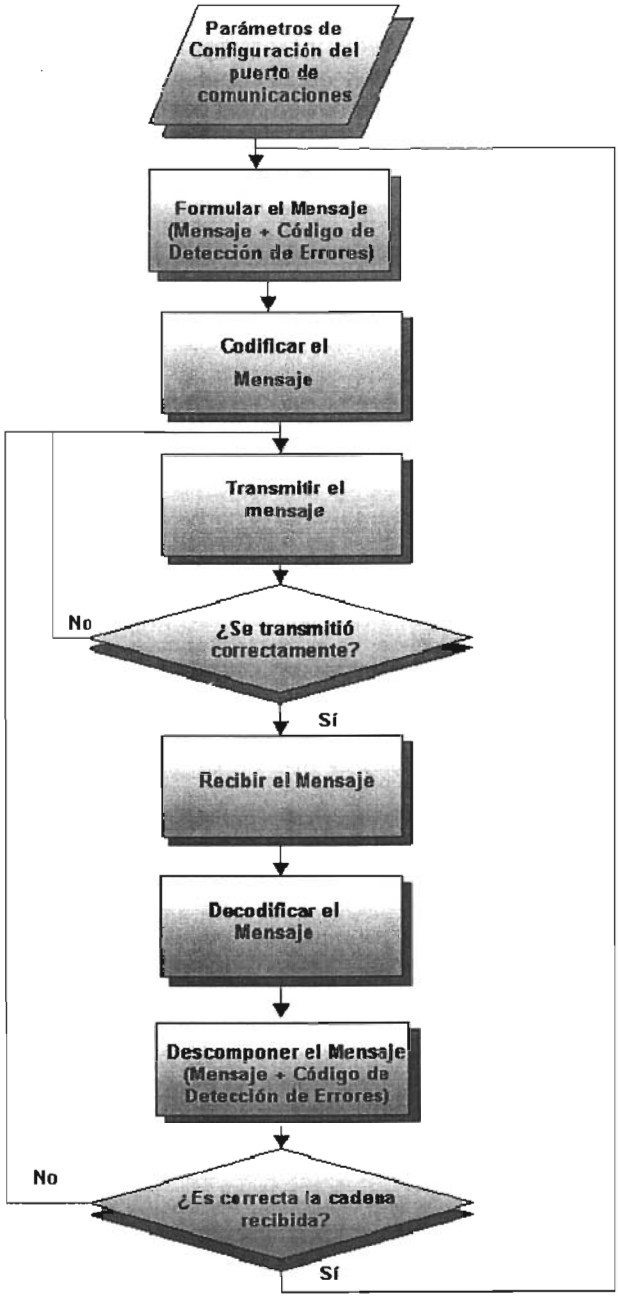


Figura 1
Diagrama de flujo básico para el módulo de Comunicaciones

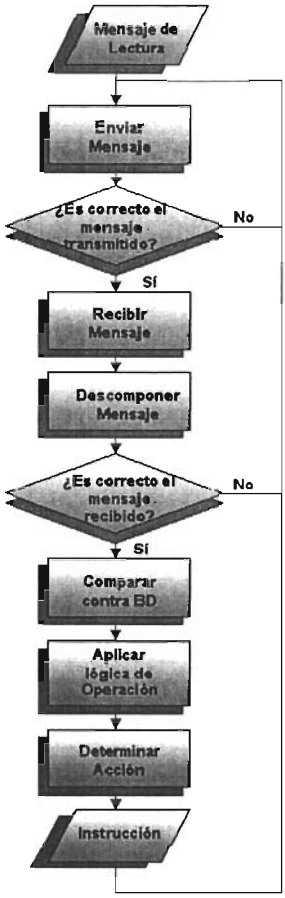


Figura 2
Diagrama de flujo del Segundo Prototipo del Módulo de Comunicaciones

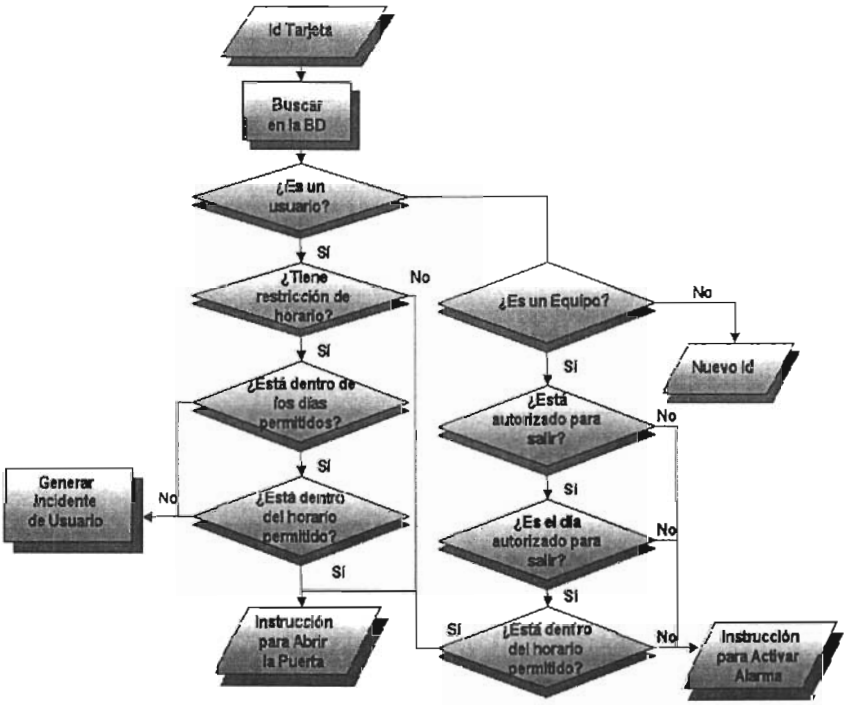


Figura 3
Diagrama de Flujo de la Lógica de Operación del Módulo de Comunicaciones

Dispositivos		Comando											
		Operación	Inicio del Mensaje	Dirección Destino	Dirección Origen	Código del Mensaje	Longitud del Mensaje	Dato 1	Dato 2	Dato3	Dato 4	CRC 1	CRC 2	Fin de Mensaje
TAG	Antena	Lectura	01	DD	DO	11	00					CRC 1	CRC 2	04
		Respuesta (Si detectó tarjeta)	01	DD	DO	01	04	ID 1	ID 2	ID 3	ID 4	CRC 1	CRC 2	04
		Respuesto (No detectó tarjeta)	01	DD	DO	01	00					CRC 1	CRC 2	04
	Dispositivos Electrónicos de Detección	Lectura Individual	01	DD	DO	33	01	Dirección Sensor				CRC 1	CRC 2	04
		Respuesta (Activo)	01	DD	DO	33	02	Dirección Sensor	01			CRC 1	CRC 2	04
		Respuesta (Inactivo)	01	DD	DO	33	02	Dirección Sensor	00			CRC 1	CRC 2	04
		Lectura General	01	DD	DO	33						CRC 1	CRC 2	04
		Respuesta General	01	DD	DO	33	01	BB				CRC 1	CRC 2	04
	Actuadores	Enceder	01	DD	DO	44	02	Dirección Actuador TAG	01			CRC 1	CRC 2	04
		Apagar	01	DD	DO	44	02	Dirección Actuador TAG	00			CRC 1	CRC 2	04
		Respuesta (Operación Correcta)	01	DD	DO	44	01	FF				CRC 1	CRC 2	04
		Respuesta (Operación Incorrecta)	01	DD	DO	44	01	CC				CRC 1	CRC 2	04
Serie 2000	Antena	Direccionar	01	DD	DO	4D	03	02	Dirección Antena	00		CRC 1	CRC 2	04
		Lectura	01	DD	DO	20	00					CRC 1	CRC 2	04
		Respuesta (Si detectó tarjeta)	01	DD	DO	20	04	ID 1	ID 2	ID 3	ID 4	CRC 1	CRC 2	04
		Respuesto (No detectó tarjeta)	01	DD	DO	20	01	40				CRC 1	CRC 2	04

Notas:

Todos los valores son dados en código Hexadecimal

DD- Dirección Lógica del Dispositivo Receptor

DO- Dirección Lógica del Dispositivo Tranmisor

Dirección Sensor- La Dirección puede estar en el rango 00-07

Dirección Actuador- La Dirección puede estar en el rango 00-07

Dirección Antena- La Dirección puede estar en el rango 00-03

BB- Valor enmascarado que representa los 8 puertos del módulo TAG.

Figura 4
Lógica del Hardware

Dispositivos			Condición	Acción	
TAG	Antena		Restringir Acceso de Personal Por hora y por fecha	Autorizado: Abrir cerradura magnética. Generar reporte de Entradas y Salidas de Usuarios	No Autorizado: Generar reporte de intento de acceso no autorizado
	Dispositivos Electrónicos de Detección	Sensor Magnético	Sin restricción	Activo: Activar Alarma Local. Generar reporte de incidentes	
			Restringir por horario y fecha	Activar Alarma General. Generar reporte de incidentes	
		Sensor de Ruptura	Sin restricción	Activar Alarma General. Generar reporte de incidentes	
		Sensor de Movimiento	Restringir por horario y fecha	Activar Alarma General Generar reporte de incidentes	
		Botón de Emergencia	Sin restricción	Generar reporte de incidentes	
		Interfón	Sin restricción	Abrir cerradura magnética.	
			Restringir por horario	Abrir cerradura magnética.	
Serie 2000	Antena		Restringir Salida de equipo por hora y fecha	Autorizado: Generar reporte de salida de Equipo.	No Autorizado: Activar Alarma General. Generar reporte

Figura 5
Lógica Operacional del Sistema

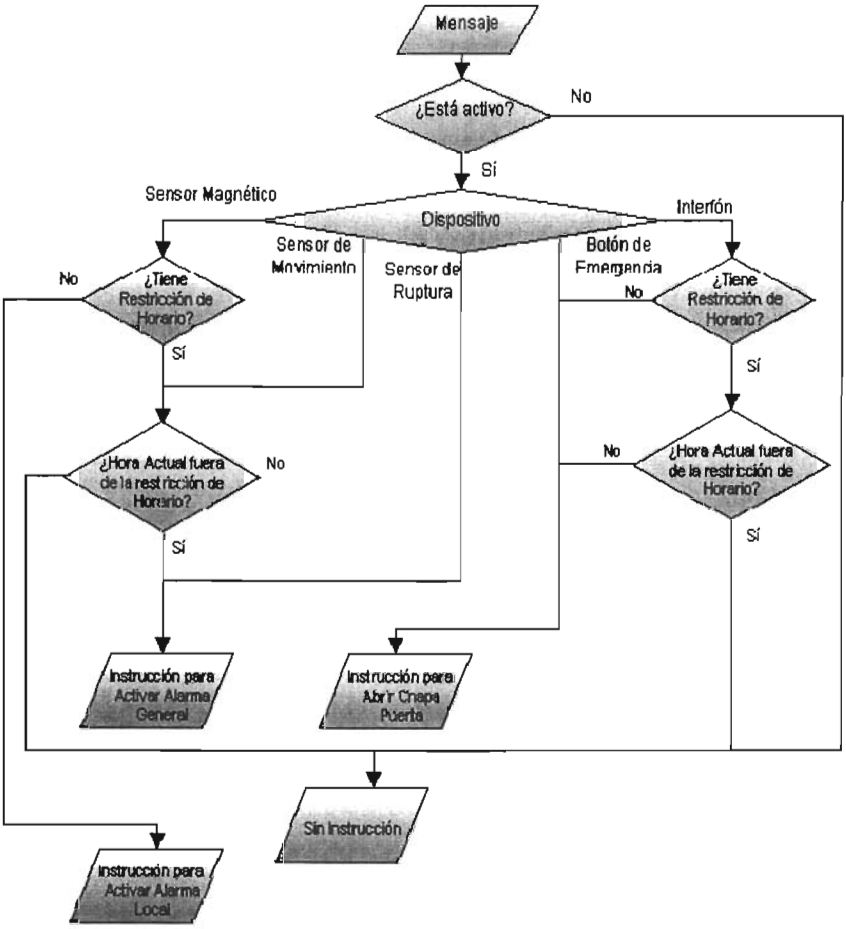


Figura 6
Diagrama de Flujo de la Lógica Operacional del Sistema

Diccionario de Datos

Tabla: ACTUADORES

Campos

Nombre	Tipo	Nulo
DIRECCION_ACTUADOR	CHAR(2)	NOT NULL
DIRECCION_MODULO	CHAR(2)	NOT NULL
TIPO_ACTUADOR	INTEGER	NOT NULL
MENSAJE	CHAR(15)	

Tabla: AREAS

Campos

Nombre	Tipo	Nulo
ID_AREA	INTEGER	NOT NULL
DESCRIPCION_AREA	CHAR(50)	

Tabla: DISPOSITIVOS

Campos

Nombre	Tipo	Nulo
DIRECCION_DISPOSITIVO	CHAR(2)	NOT NULL
DIRECCION_MODULO	CHAR(2)	NOT NULL
TIPO_DISPOSITIVO	INTEGER	NOT NULL
MENSAJE	CHAR(15)	
LOGICA_ACTIVACION	CHAR(1)	
HORA_INICIAL	TIME	
HORA_FINAL	TIME	
DIA_INICIAL	DATE	
DIA_FINAL	DATE	
LOGICA_ACCION	SMALLINT	
SABADO	SMALLINT	
DOMINGO	SMALLINT	

Tabla: MODULOS

Campos

Nombre	Tipo	Nulo
DIRECCION_MODULO	CHAR(2)	NOT NULL
TIPO_MODULO	SMALLINT	NOT NULL
ID_AREA	INTEGER	NOT NULL

Tabla: TIPO_ACTUADORES

Campos

Nombre	Tipo	Nulo
TIPO_ACTUADOR	INTEGER	NOT NULL
DESCRIPCION_ACTUADOR	CHAR(50)	
TIPO_MODULO	SMALLINT	

Tabla: TIPO_DISPOSITIVOS

Campos

Nombre	Tipo	Nulo
TIPO_DISPOSITIVO	INTEGER	NOT NULL
DESCRIPCION_DISPOSITIVO	CHAR(50)	
TIPO_MODULO	SMALLINT	

Tabla: TIPO_MODULOS

Campos

Nombre	Tipo	Nulo
TIPO_MODULO	SMALLINT	NOT NULL
DESCRIPCION_MODULO	CHAR(50)	

```
SET TERM!!;
CREATE PROCEDURE VALIDA_USUARIO (
   ID_USUARIO CHAR(20) CHARACTER SET NONE,
   HORA TIME,
   DIA INTEGER,
  FECHA DATE,
   AREA INTEGER)
RETURNS (
   VALIDACION SMALLINT,
   USUARIO CHAR(20) CHARACTER SET NONE)
AS
DECLARE VARIABLE RES SMALLINT;
DECLARE VARIABLE USUARIO1 SMALLINT;
BEGIN
 FOR SELECT RESTRICCION,ID_USUARIO FROM USUARIOS_RESTRICCION
 WHERE USUARIOS_RESTRICCION.ID_USUARIO=:id_usuario
 INTO :res, :usuario
 DO
  BEGIN
   IF(:res IS NULL) THEN
    BEGIN
    validacion='2';
    END
   ELSE
    BEGIN
    IF (:res ='0')THEN
    BEGIN
    EXECUTE PROCEDURE  REGISTRAR_ACCESO_USUARIO(:id_usuario,:hora,
    :fecha, :area);
    validacion='1';
    END
    ELSE
    BEGIN
     FOR SELECT COUNT(*) FROM USUARIOS_HORARIOS,HORARIOS
     WHERE (HORARIOS.HORA_I <= :hora AND :hora < HORA_F)
     AND USUARIOS_HORARIOS.ID_USUARIO IN
      (SELECT ID_USUARIOS FROM USUARIOS_DIAS
       WHERE USUARIOS_DIAS.ID_DIAS=:dia
       AND USUARIOS_DIAS.ID_USUARIOS IN
         (SELECT ID_USUARIO FROM USUARIOS_AREAS
          WHERE USUARIOS_AREAS.ID_AREA=:area
          AND USUARIOS_AREAS.ID_USUARIO=:id_usuario))
    INTO :usuario1
    DO
    BEGIN
     IF(:usuario1 ='0' ) THEN
       BEGIN
EXECUTE PROCEDURE REGISTRAR_ACCESO_USUARIO(:id_usuario, :hora, : fecha, : area);
       validacion='0';
       END
     ELSE
     BEGIN
EXECUTE PROCEDURE REGISTRAR_ACCESO_USUARIO(:id_usuario,:hora, :fecha, :area);
      validacion ='1';
     END
     END
    END
   END
  END
 EXIT;
END !!
SET TERM; !!
```

Figura 1
Procedimiento Almacenado "Valida usuario"

```
SET TERM !! ;
    CREATE PROCEDURE REGISTRAR_ACCESO_USUARIO(id_usuario CHAR(20), hora_es TIME, fecha_es DATE,
area_acceso CHAR(1))
    AS
      DECLARE VARIABLE hora TIME;
      BEGIN
         FOR SELECT MAX(HORA_ENTRADA) FROM REGISTRO_ES_USUARIOS
         WHERE (ID_USUARIO= :id_usuario) AND (FECHA= :fecha_es)
         AND (HORA_SALIDA IS NULL)
         INTO :hora
         DO
          BEGIN
            IF (:hora IS NULL) THEN
              BEGIN
                INSERT INTO REGISTRO_ES_USUARIOS(ID_USUARIO,HORA_ENTRADA,FECHA,AREA)
                VALUES( :id_usuario, :hora_es, :fecha_es, :area_acceso);
              END
            ELSE
              BEGIN
                UPDATE REGISTRO_ES_USUARIOS SET HORA_SALIDA= :hora_es
                WHERE (ID_USUARIO= :id_usuario) AND (FECHA= :fecha_es)
                AND (HORA_SALIDA IS NULL);
              END
          END
      EXIT;
      END !!
SET TERM ; !!
```

Figura 2
Procedimiento Almacenado "Registrar acceso usuario"

```
SET TERM !! ;
    CREATE PROCEDURE REGISTRAR_INCIDENTE_USUARIO(id_usuario CHAR(20),hora TIME, fecha DATE,area_inc
CHAR(1))
    AS
      BEGIN
         INSERT INTO
INCIDENTES_USUARIOS(ID_USUARIO,HORA_INCIDENTE,FECHA_INCIDENTE,TIPO_INCIDENTE,AREA)
         VALUES(:id_usuario, :hora, fecha,'9',:area_inc);
      EXIT;
      END !!
SET TERM ; !!
```

Figura 3
Procedimiento almacenado "Registrar Incidente Usuario"

```
SET TERM !! ;
    CREATE PROCEDURE VALIDA_EQUIPO(id_equipo CHAR(20), fecha DATE, hora_inicial TIME, hora_final TIME,
    hora_actual TIME, area SMALLINT)
    RETURNS(VALIDACION SMALLINT, ID CHAR(20))
    AS
      DECLARE VARIABLE sal SMALLINT;
      BEGIN
          FOR SELECT SALIDA, ID_SALIDA_EQUIPO FROM SALIDA_EQUIPO
          WHERE (ID_SALIDA_EQUIPO = :id_equipo)
          INTO :sal, :id
          DO
           BEGIN
             IF(:sal= '0') THEN
               BEGIN
                EXECUTE PROCEDURE REGISTRAR_INCIDENTE_EQUIPO(:id_equipo, hora_actual, fecha, 4', :area);
                VALIDACION = '0';
               END
             ELSE
               BEGIN
                IF (:sal = '1') THEN
                  BEGIN
                   FOR SELECT ID_CONTROL_SALIDA_EQUIPO FROM CONTROL_SALIDA_EQUIPO
                   WHERE (DIA_AUTORIZADO = :fecha)
                   AND (HORA_AUTORIZADA BETWEEN :hora_inicial AND :hora_final)
                   AND (ID_CONTROL_SALIDA_EQUIPO = :id_equipo)
                   INTO :id
                   DO
                     BEGIN
                       IF (:id IS NULL)THEN
                          BEGIN
                             VALIDACION = '';
                          END
                       ELSE
                          BEGIN
                             EXECUTE PROCEDURE REGISTRAR_SALIDA_EQUIPO(:id_equipo, :hora_actual, fecha);
                             VALIDACION = '1';
                          END
                     END
                  END
                ELSE
                  BEGIN
                    VALIDACION = '2';
                  END
               END
           END
      EXIT;
      END !
```

Figura 4
Procedimiento almacenado "Valida Equipo"

```
SET TERM !! ;
    CREATE PROCEDURE REGISTRAR_SALIDA_EQUIPO(id CHAR(20),hora TIME, fecha DATE)
    AS
      BEGIN
          UPDATE REGISTRO_ES_EQUIPO SET HORA_SALIDA = :hora,FECHA_SALIDA = :fecha
          WHERE (FECHA_SALIDA IS NULL) AND ID_EQUIPO = :id ;
      EXIT;
      END !!
SET TERM ; !!
```

Figura 5
Procedimiento almacenado "Registrar salida equipo"

```
SET TERM !! ;
    CREATE PROCEDURE REGISTRAR_INCIDENTE_EQUIPO(id_equipo CHAR(20),hora TIME, fecha DATE,tipo
SMALLINT, area_inc CHAR(1))
    AS
      BEGIN
          INSERT INTO
INCIDENTES_EQUIPO(ID_EQUIPO,HORA_INCIDENTE,FECHA_INCIDENTE,TIPO_INCIDENTE,AREA)
          VALUES(:id_equipo,:hora,:fecha,:tipo,:area_inc);
      EXIT;
      END !!
SET TERM ; !!
```

Figura 6
Procedimiento almacenado "Registrar incidente equipo"

```
SET TERM !! ;
CREATE PROCEDURE ACTIVA_DISPOSITIVO (dir_modulo CHAR(2), dir_dispositivo CHAR(2), hora TIME, dia
DATE, sd CHAR(1))
        RETURNS (tipoD integer)
        AS
                DECLARE VARIABLE hr_inicial TIME;
                DECLARE VARIABLE hr_final TIME;
        BEGIN
                FOR SELECT HORA_INICIAL, HORA_FINAL FROM DISPOSITIVOS
        WHERE DIRECCION_MODULO= :dir_modulo AND DIRECCION_DISPOSITIVO= :dir_dispositivo
                INTO :hr_inicial, :hr_final
                DO
                        BEGIN
                                IF (:hr_inicial > hr_final) THEN
                                        BEGIN
                            SELECT TIPO_DISPOSITIVO
                                        FROM DISPOSITIVOS
                                       WHERE
                                ( ((HORA_INICIAL <= :hora AND :hora <= CAST('23:59:59' AS TIME))
                                 OR (CAST('00:00:00' AS TIME)<= :hora AND :hora <= HORA_FINAL ) )
                                 OR (DIA_INICIAL <= :dia AND :dia <= DIA_FINAL)
                                 OR (SABADO= :sd)
                                OR (DOMINGO= :sd))
                                 AND (DIRECCION_MODULO = :dir_modulo)
                               AND (DIRECCION_DISPOSITIVO = :dir_dispositivo)
                                        INTO :tipoD;
                                                END
                                    ELSE
                          SELECT TIPO_DISPOSITIVO
                                        FROM DISPOSITIVOS
                                        WHERE
                         ((HORA_INICIAL <= :hora AND :hora <= HORA_FINAL)
                          OR (DIA_INICIAL <= :dia AND :dia <= DIA_FINAL)
                          OR (SABADO= :sd)
                           OR (DOMINGO= :sd))
                          AND (DIRECCION_MODULO = :dir_modulo)
                        AND (DIRECCION_DISPOSITIVO = :dir_dispositivo)
                                        INTO :tipoD;
                                        END

END !!

SET TERM ; !!
```

Figura 7
Procedimiento almacenado "Activa Dispositivos"

Lógica de acción del sistema

```
Select Case dispositivo

        Case 1  'Es un Serie 2000
         tipoActuador = 3
         If Len(dato) > 2 Then  'Leyo un equipo
             '*****************  PROCEDIMIENTO DEL SERIE 2000 **********
             strSQLCom = "EXECUTE PROCEDURE VALIDA_EQUIPO('" & dato & "'," & _
             "'" & dia & "', '" & Format(hr_min, "hh:mm:ss") & "', '" & Format(hr_max, "hh:mm:ss") & "'," & _
          "'" & Format(hr, "hh:mm:ss") & "', " & area & ")"
          Set rsCom = connCom.Execute(strSQLCom)

            '******************  LOGICA DEL SERIE 2000 ******************
          If  IsNull(rsCom!id) Then 'Si el id no existe en la base de datos
                    'Text2.Text = "Nuevo ID"
                             nuevoEquipo = dato
          Else
                     If rsCom.EOF Then '" Activamos Alarma General"
    strSQLCom = "EXECUTE PROCEDURE REGISTRAR_INCIDENTE_EQUIPO('" & dato & "','" & Format(hr,
    "hh:mm:ss") & "','" & dia & "','4','" & area & "')"

                    connCom.Execute strSQLCom
                    Call agrega_actuador_activo(tipoActuador, 1)
                    Nodos.Activo(nodo) = True
                    Call cargaImagenSensores(nodo, 1)
                     Else
                     Select Case rsCom!validacion
                    Case 0  '"Alarma General"
                              Call agrega_actuador_activo(tipoActuador, 1)
                              Nodos.Activo(nodo) = True
                     Case 1 '"Salida autorizada"
                              'Mensaje de salida de equipo
                    Case 2  '"Devolucion de equipo"
                                       'Mensaje de devolucion de equipo
                    End Select
                    End If
          End If
          strSQLCom = "commit"
          connCom.Execute strSQLCom
                                '*****************************************************************
       End If

    Case 2  'Es un TAG, validamos el usuario
          If Len(dato) > 2 Then 'Leyó la credencial de un usuario
                    tipoActuador = 1 & area

                    '*****************  ALARMA GENERAL  ****************************
                    'If NodoActuador.Activo(3 & area) = True Then Exit Function 'Si esta activa la alarma  general,
          no abras puertas
          '*****************************************************************

          '*****************     EJECUTAMOS EL PROCEDIMIENTO  ***************************
           strSQLCom = "EXECUTE PROCEDURE VALIDA_USUARIO('" & dato & "'," & _
           "'" & Format(hr, "hh:mm:ss") & "'," & _
           "'" & dia & "', '" & num_dia & "','" & area & "')"
          Set rsCom = connCom.Execute(strSQLCom)

          '*******************  LOGICA DEL TAG  ***********************************************
          If IsNull(rsCom!usuario) Then 'Si el id no existe en la base de datos
                    'Text4.Text = "Nuevo ID"
                    nuevoId = dato
           Else
             If (IsNull(rsCom!validacion)) Then
                    '"Acceso no autorizado"
                  strSQLCom = "EXECUTE PROCEDURE REGISTRAR_INCIDENTE_USUARIO('" & dato &
                  "','" & Format(hr, "hh:mm:ss") & "','" & dia & "','" & area & "')"
```

```
            connCom.Execute strSQLCom
          Else
            Call agrega_actuador_activo(tipoActuador, 1)
            tmrCerraduraMagnetica(area - 1).Interval = tiempo_puertas(area - 1)
            Nodos.Activo(nodo) = True
            Call frmPrincipal.ActualizaRegistrosESUsuarios
          End If
        End If
        strSQLCom = "commit"
        connCom.Execute strSQLCom

    End If
'*****************************************************************************

Case 3 'Sensor de Movimiento
    'Ejecutar procedimiento para ver si checamos o no el sensor de movimiento
    tipoActuador = 3 & area
    '********************  PROCEDIMIENTO SENSORES  ******************************
    strSQLDispositivos = "execute procedure activa_dispositivo('" & dir_m & "','" & dir_d & "','" &
    TimeValue(hr) & "','" & lblFecha.Caption & "','" & num_dia & "')"
    Set rsDispositivos = connDispositivos.Execute(strSQLDispositivos)
    '*********************LOGICA DEL SENSOR DE MOVIMIENTO  ************************
    If Not IsNull(rsDispositivos!tipod) Then 'Debe ser revisado
      If NodoActuador.Activo(tipoActuador) = False Then
        Call agrega_actuador_activo(tipoActuador, 1)
        Nodos.Activo(nodo) = True
        Call cargaImagenSensores(nodo, 1)
        Call genera_reporte(nodo, area, 3, 3)
      End If
    End If

Case 4 'Es un sensor de Ruptura
    'Verificamos si se encuentra dentro del horario

    '********************  PROCEDIMIENTO  ******************************
    strSQLDispositivos = "execute procedure activa_dispositivo('" & dir_m & "','" & dir_d & "','" &
    TimeValue(hr) & "','" & lblFecha.Caption & "','" & num_dia & "')"
    Set rsDispositivos = connDispositivos.Execute(strSQLDispositivos)
    '******************** LOGICA DEL SENSOR DE RUPTURA ***********************
    tipoActuador = 3 & area
    If Not IsNull(rsDispositivos!tipod) Then 'Debe activarse
      If NodoActuador.Activo(tipoActuador) = False Then
        Call agrega_actuador_activo(tipoActuador, 1)
        Nodos.Activo(nodo) = True
        Call genera_reporte(nodo, area, 2, 3)
        Call cargaImagenSensores(nodo, 1)
      End If
    End If

Case 5 'Es un sensor magnético para las puertas
        strSQLDispositivos = "execute procedure activa_dispositivo('" & dir_m & "','" & dir_d & "','" &
        TimeValue(hr) & "','" & lblFecha.Caption & "','" & num_dia & "')"
        Set rsDispositivos = connDispositivos.Execute(strSQLDispositivos)
    If IsNull(rsDispositivos!tipod) Then 'No deberia estar abierto
      If NodoActuador.Activo(1 & area) = False Then 'La puerta debe estar cerrada
        tipoActuador = 2 & area
        If NodoActuador.Activo(tipoActuador) = False Then
          Call agrega_actuador_activo(tipoActuador, 1)
          Nodos.Activo(nodo) = True
          Call genera_reporte(nodo, area, 1, 2)
          Call cargaImagenSensores(nodo, 1)
        End If
      End If
    End If

Case 6 'Es un interfón
```

```
            tipoActuador = 1 & area
              strSQLDispositivos = "execute procedure activa_dispositivo('" & dir_m
            & "','" & dir_d & "','" & TimeValue(hr) & "','" & lblFecha.Caption & "','"
            & num_dia & "')"

        Set rsDispositivos = connDispositivos.Execute(strSQLDispositivos)
        If Not rsDispositivos.EOF Then 'Puedo abrir la puerta
          If NodoActuador.Activo(tipoActuador) = False Then
              Call agrega_actuador_activo(tipoActuador, 1)

            tmrCerraduraMagnetica(area - 1).Interval = tiempo_puertas(area - 1)
            Nodos.Activo(nodo) = True
            Call genera_reporte(nodo, area, 15, 1)
          End If
        End If

    Case 7 'Es un botón de emergencia
      tipoActuador = 2 & area
        If NodoActuador.Activo(tipoActuador) = False Then
          NodoActuador.Activo(tipoActuador) = True
          Call genera_reporte(nodo, area, 10, 2)
          Nodos.Activo(nodo) = True
          Call cargaImagenSensores(nodo, 1)
        End If

    Case 8 ' Es un sensor magnético para los zaguanes
        strSQLDispositivos = "execute procedure activa_dispositivo('" & dir_m & "','" & dir_d & "','" &
        TimeValue(hr) & "','" & lblFecha.Caption & "','" & num_dia & "')"
        Set rsDispositivos = connDispositivos.Execute(strSQLDispositivos)
        If IsNull(rsDispositivos!tipod) Then 'No deberia estar abierto
        'Activo alarma general
            tipoActuador = 3 & area
            If NodoActuador.Activo(tipoActuador) = False Then
              Call agrega_actuador_activo(tipoActuador, 1)
              Nodos.Activo(nodo) = True
              Call genera_reporte(nodo, area, 1, 3)
              Call cargaImagenSensores(nodo, 1)
            End If
        End If

    Case Else
End Select
```