14

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

SISTEMA DE IDENTIFICACION Y CONTROL DE ACCESO DE PERSONAL EN LINEA

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

P R E S E N T A N :

BARRERA PACHECO ROBERTO CARLOS

CANUTO CARRANCO JORGE ANTONIO

CHAVEZ PAZ CARLOS

ASESOR: ING GLORIA MATA HERNANDEZ

MEXICO, D. F. 2002

DEDICATORIAS

A mi hijita hermosa, cuyo tiempo de jugar me regaló en los momentos de trabajo, sin pedirme nada a cambio más que un beso.

A mi madre, que con cariño y amor me da ejemplo diario de abnegación en todos mis actos.

A mi admirable padre, cuya figura responsable, paciente, sabia y llena de amor ha sido y será por siempre el modelo de vida honesta a seguir.

A mi amada esposa, mi cariñito, por su tierno apoyo, paciencia y comprensión que me brindó durante mi trabajo y que me da siempre en todo momento.

A mis tres hermanas, aquellas flores que dieron mucha vida y color al jardín de mi niñez.

Jorge Antonio

A mi alma Máter: la U.N.A.M.

Al Colegio de Ciencias y Humanidades Plantel Sur.

A la Facultad de Ingeniería: sembradora de Heraldos de la Física.

A mi directora de Tesis: La Ing. Gloria Mata Hernández.

A mis padres(Martha y Roberto): En retribución al buen camino por el cual me han sabido guiar a lo largo de mi vida.

A Rafael, Arturo, Edgar, Claudia y Erika: Mis queridos hermanos, por el ejemplo de lucha por la vida que me han dado.

A mis adorables sobrinos, con todo cariño: Samantha, Dante Arturo, Liza Esther, Joselú y Erika Lebón.

A mis tíos, primos y cuñados.

A mi abuelo Roberto con todo respeto y cariño.

A los que se nos adelantaron en el camino: Mis abuelitos: Leonardo, Ramona, Tomasa y Julia. Mi tío: Arturo.

A mis vecinos y amigos: En especial a Miguel Salgado, Jorge Andrade, a Lorena y a mis amigos de la Presidencia y de anteriores empleos.

A Yuri mi amiga y jefa: Por ese alto sentido de la organización y responsabilidad. Por el apoyo que me has dado en esta difícil empresa.

A mis amigos de la infancia y adolescencia.

Roberto Carlos

A mis padres, por darme todos mi valores y principios, por brindarme todo su amor y cariño, pero sobre todo, por el esfuerzo que hicieron dia con dia para que pudiera terminar una carrera. Padres, esto es suyo.

A mis hermanos; Margarita, Rosario, Lilia y Octavio por cuidarme, guiarme y apoyarme en todos los dias de mi vida, los quiero mucho.

A mis sobrinos, Sergio, Manuel, Luis, Berenice, por iluminar nuestras vidas.

A mis cuñados: Norma y Jacinto, por integrarse a mi familia.

A la Lic. Pilar López Tena, por creer en mi y brindarme su amistad.

Al Ing. Héctor de Santiago Ramírez, por todo el apoyo brindado para el desarrollo de esta tesis.

A mis amigos y compañeros de la Universidad Panamericana: Alfredo, Alejandro, Anilú, Bernardo, Fabián, Paola y Rodolfo, y todos aquellos que me soportaron todos los días.

A la Universidad Nacional Autónoma de México, en especial a la Facultad de Ingeniería por darme el honor de estudiar en sus aulas.

A mis compañeros de tesis Roberto y Jorge, en especial a Roberto Urbina y Roberto Montaño.

A mis amados hijos: Mariana y Diego, que con sus sonrisas y besos, me dieron la fuerza necesaria para terminar este trabajo. Los quiero mucho.

A la mujer que siempre estuvo motivándome todos los dias, Pilar, mi querida esposa, quién nunca perdió la fe en mi. Gracias por estar conmigo y darme unos hijos maravillosos.

A ti, por darme todo lo bueno que tengo en esta vida: DIOS.

Carlos

ÍNDICE

INTRODUCCIÓN

En la actualidad, existen empresas e instituciones que cuentan con sistemas de control de acceso que les permite llevar de manera más o menos eficiente el manejo del personal que labora en sus instalaciones, debido a que estos sistemas son centralizados; es decir, es necesario mantenerlos en un solo lugar para poder llevar a cabo esa tan importante labor. Esto se torna aún más complicado cuando las instalaciones son relativamente amplias, razón por la cual es necesario contar con puestos de control en áreas específicas, los cuales, debido a su mala comunicación no mantienen el nivel de control tan óptimo como se requiera. Ahora bien, si existe la necesidad de supervisar al personal que tiene ciertas responsabilidades vitales dentro de la empresa o institución, sin estar presente, o bien, recabar información general relacionada a la identificación del personal como:

- Asegurarse que el personal de seguridad recorre las instalaciones durante el transcurso de la noche.
- Si se encuentra personal no autorizado en áreas restringidas de la empresa.
- Localizar a personal dentro de la empresa.
- Realizar estadísticas del personal relacionadas con los accesos al centro de trabajo.

Es conveniente contar con un instrumento que permita la detección, control y monitoreo del personal en una empresa de una manera ágil, rápida y segura. Los sistemas de control de acceso que se pueden definir como sistemas de identificación que utilizan las empresas para proteger el ingreso a recintos y aplicaciones y aunque, tradicionalmente, se han asociado a soluciones basadas en tarjetas magnéticas, también existen otras tecnologías como la identificación biométrica que a través de un lector verifica la identidad de una persona comparando esos datos con aquellos que están guardados en una base de datos o en una tarjeta inteligente.

Evolución de los dispositivos de identificación

Las primeras formas de identificación se realizaban asignando a las personas un "medio identificador" que debían llevar consigo para presentarlo ante el personal a cargo de la seguridad del inmueble, el cual registraba cada acceso en una bitácora de eventos (normalmente una libreta), para que posteriormente (al surgir un imprevisto) se realizara una consulta para la toma de decisiones

Tiempo después al acelerarse la era de la miniaturización del chip, las personas fueron dotadas ahora de otro "medio identificador" que debían presentar ante el lector de un equipo, ya sea una tarjeta magnética, de código de barras, de proximidad, una pastilla de identificación u otros, de forma tal que éstos pudieran distinguir entre diferentes tarjetas al ser pasadas por el lector y así diferenciar una persona de otra

Esta forma de identificación, aunque efectiva, es necesario complementarla con algunas políticas de utilización (no permitir el préstamo de las tarjetas, la tarjeta es personal, etc.) debido a que no es una identificación real del individuo, ya que basta con que una persona

tenga en su poder el medio de identificación de otra, para tener acceso a las instalaciones. Una posible solución a este problema es el agregado de una clave personal asociada al medio de identificación, por lo cual además de poseer el medio, se necesitará también conocer la clave personal. Este tipo de identificación es el más utilizado en la actualidad debido a su costo accesible y fácil utilización.

La mejor forma de asegurar la identificación real de las personas fue puesta en marcha en la década de los 90's, donde el medio de identificación es la persona misma o una de sus características físicas, las cuales deben ser diferentes y propias de cada persona. Ante esta necesidad, surge el desarrollo de una nueva tecnología que se llamó biométrica, debido a que se miden (métrica) características biológicas (bio) de los individuos.

Algunas de las tecnologías que existen actualmente son:

- Huella digital
- Geometría de mano
- Iris del ojo
- Geometría de dedos

Cada una de estas cuatro tecnologías posee capacidades diferentes, tornándose adecuadas para su utilización específica en diferentes situaciones. Sin embargo, cabe aclarar que la verificación por biometría es una de las más costosas de implementar.

Elementos en un sistema de control de accesos

Cuando hablamos de los sistemas de Control de Accesos, lo primero que vamos a necesitar definir es el requerimiento específico al problema en cuestión, lo podemos resolver con equipos Abre Puertas autónomos o si necesariamente debemos instalar un Sistema de Control de Accesos Integral. Es fácil llegar a saberlo porque el uso de un Abre Puertas Inteligente autónomo, se da generalmente para los casos de controles pequeños, de pocas puertas (quizás una sola) y donde lo único que se pretende es limitar el ingreso de personas no autorizadas a un determinado recinto (generalmente un centro de cómputos, un laboratorio, etc.), sin importar demasiado obtener información respecto a los eventos que se han producido en ese acceso. Sin embargo, cuando se instala un Sistema de Control de Acceso, todo el equipo involucrado está conectado entre sí y se centraliza todo la información y supervisión del sistema en una computadora, que tendrá instalado un Software de Gestión, Administración, Control y Supervisión de todos los accesos, facilitando así que cualquier puesto de control pueda tener información confiable al instante.

A continuación, iremos detallando algunos elementos, que se utilizan para sistemas de control, explicando las características de cada uno brevemente y finalizaremos sintetizando todo, en una tabla comparativa.

Acceso por Tarjeta de Proximidad

Tipo de tarjeta.- Es una tarjeta que por su diseño tecnológico, es difícil de duplicar. Permite utilizar tarjetas o llaveros de proximidad pasivos. La tarjeta no tiene rozamiento (se comunica con el equipo por radio frecuencia), por lo cual no se desgasta. Hoy en día es una de las tecnologías más moderna y efectiva, por su versatilidad y bajo costo de mantenimiento. Tiene un costo medio, sin embargo su duración hace que resulte, la más económica, porque no requiere recambios por desgastes.

Lector: El dispositivo abre puertas electrónico P-LOCK reemplaza a las llaves convencionales, permitiendo controlar en forma más efectiva el acceso a edificios, oficinas, garajes, etc.

Acceso por Tarjeta de Código de Barras

Tipo de tarjeta: Es una tarjeta de apariencia similar a la magnética, pero en lugar de la banda, lleva impreso un código de barras, el cual puede incluso ser protegido con una banda protectora (código oculto) que evita la duplicación de la tarjeta por fotocopias. La ventaja de esta tarjeta, es que al pasarla por el lector, no existe rozamiento, sólo hay un haz de luz que lee el código en cuestión, con lo cual su vida útil es levemente mayor. No hay que olvidar tampoco que no se pueden rayar, porque de esa forma se altera o incluso llega a hacerse ilegible el código, obligando al cambio de tarjeta. El costo de las tarjetas es similar a las magnéticas.

Lector: Permite utilizar tarjetas de código visible o código oculto. Además el lector es multicódigos, permitiendo el uso de tarjetas con códigos UPC, 2 de 5, 3 de 9, etc. Dado, como ya dijimos, que no hay rozamiento, su duración es superior al magnético, aunque no tanto como uno de proximidad o touch memory. Su costo es intermedio entre uno magnético y uno de proximidad.

Acceso por Tarjeta Magnética

Tipo de tarjeta: Es la más conocida y difundida, dado que se utiliza en todos los sistemas de tarjetas crédito y de compra. Su ventaja es su difusión, popularidad y el bajo costo, pero en sí es, de todos los medios de identificación, el más vulnerable de todos. Su banda magnética, debe ser tratada con cierto cuidado, para evitar que se raye o sea expuesta a campos magnéticos que la borren, por tal motivo, no son recomendables para usar en ambientes industriales. Sólo se recomiendan en oficinas o establecimientos administrativos.

Lector: El lector de tarjetas magnéticas, permite leer cualquier tarjeta magnética estándar grabada en ABA Track 2, inclusive las tarjetas de crédito o compra que existen en el mercado.

En relación con el lector en sí, (si bien es económico) posee un cabezal magnético, el cual sufre cierto desgaste al pasar las tarjetas por el lector. En realidad cada tarjeta que se pasa, deja micro partículas depositadas sobre la cabeza lectora. Ahora bien, si esas partículas son abrasivas, comienzan a rayar las tarjetas sucesivas y las tarjetas rayadas o rotas, deterioran aun más el cabezal, obligando al recambio del lector y de las tarjetas dañadas. El tiempo de duración, depende exclusivamente del ambiente, frecuencia de uso y el trato con el que se les utilice, pero el promedio está entre 9 meses y 3 años.

Ingreso por contacto por memorias (Touch Memories)

Tipo de tarjeta: El elemento es una pastilla electrónica, encapsulada en acero inoxidable de unos 16 mm de diámetro, que se transporta con un soporte plástico de unos 5 cm de largo con un orificio en su parte superior para poder colgarlo en un llavero. Comúnmente se les denomina llave electrónica. Brindan un muy alto nivel de confiabilidad, ya que son altamente resistentes al desgaste, siendo ideales para ambientes industriales en donde la probabilidad de falla, vandalismo o sabotaje sea alta, aunque no son recomendables para ambientes con alto grado de generación de corriente estática (por ejemplo: oficinas con mucha alfombra y ambientes muy secos). Su tecnología de avanzada evita la posibilidad de duplicarlas. Realmente muy confiables. En precio son unos de los medios más caros, aunque en relación (salvo que alguien lo pierda) nunca se desgastan, como puede suceder con una tarjeta, con lo cual a largo plazo resulta conveniente.

Lector: El lector es también de acero inoxidable y por ende no tiene desgaste con el uso. Es el más económico de toda la línea.

Acceso biométrico

Su funcionamiento se basa en la lectura de alguna parte del cuerpo humano, eliminando por completo el uso de las tarjetas. Su principal ventaja radica en la seguridad, ya que por su esencia nadie puede entregarle o pedirle a otra persona la "tarjeta para checar o pasar", pero hasta el momento siguen luchando para resolver varios puntos que complican su entrada masiva al mercado. El más importante pasa por el precio del lector, y le siguen la velocidad de lectura (comúnmente son bastante lentos o deben ir acompañados de un teclado para anteponer un código para acelerar el proceso de búsqueda), y por último la poca posibilidad de ser autónomos (generalmente por su complicada lógica se ven obligados a trabajar con un software de análisis y una PC conectada directa al lector, lo cual es poco versátil y más caro aún), pero seguramente con el tiempo se irán superando estas dificultades y en un futuro de mediano plazo, llegarán a ser un estándar más.

Lector: Los más conocidos pueden ser los lectores de Huellas Digitales, Geometría de la Mano e Iris del Ojo.

En la Tabla 1 se pueden observar las diferencias entre las características de los sistemas de identificación.

	Magnético	Código de Barras	Proximidad	Contacto por Memorias	Biométricos
Confiabilidad	Media-Baja	Media / baja	Alta	Alta	Muy Alta
Desgaste de Tarjeta	Alto	Medio / bajo	No Posee	No Posee	No Posee
Desgaste del lector	Muy Alto	Bajo	No Posee	No Posee	Bajo
Costo del mantenimiento	Alto	Medio	No Posee	No Posee	Alto
Precio de la Tarjeta	Bajo	Bajo	Medio	Medio / alto	No Posee
Precio del Lector	Bajo	Bajo	Medio	Muy Bajo	Muy Bajo

Tabla 1
Tabla comparativa de los sistemas de identificación

Tecnologías Web

La Internet se puede definir como un conjunto de redes de computadoras y equipos físicamente unidos mediante cables que conectan puntos de todo el mundo. Esta gigantesca Red se difumina en ocasiones, porque los datos pueden transmitirse vía satélite, fibra óptica o microondas, a través de ruteadores, los cuales, permiten el envío de paquetes de información a su destino buscando siempre el camino más óptimo.

Aunque la aparición de Internet data de la década de los 60's, no fue sino hasta finales de 1993 cuando presentó un crecimiento exponencial, debido tanto a la expansión de sus fronteras (limitadas únicamente al sector gubernamental y escolar), así como a la aparición de la PC de escritorio.

La propia extensión de Internet a todos los ámbitos ha popularizado el uso de los sistemas distribuidos o sistemas de 3 capas. Muchos de estos sistemas tienen requisitos de disponibilidad y tolerancia a fallas estrictas. Existen multitud de sistemas que deben de estar funcionando las 24 horas del día, los 365 días del año.

Los aspectos fundamentales de un sistema distribuido para un desarrollo sobre Internet son:

- *El servidor de base de datos*. Incluye a todos los objetos encargados de mantener la integridad referencial de la información, así como su almacenamiento, de una manera segura, para su recuperación y mantenimiento adecuados.
- *Uno o varios servidores de aplicaciones*. Contienen las Reglas del negocio, la lógica del funcionamiento del sistema, políticas y restricciones.
- *Los clientes*. Interactúan con el sistema mediante una Interfaz de usuario (UI: User Interface o Interfaz de Usuario) que generalmente es el visualizador de Internet.

Existen diversas plataformas para el desarrollo de sistemas distribuidos, Windows NT 4.0 y ahora la plataforma de Windows 2000, dichos sistemas operativos fueron desarrollados por la compañía Microsoft y actualmente se encuentran catalogados como los más populares en el mercado, esto gracias a la interfaz amigable de administración con la que cuentan, incluyendo su robustez y seguridad.

Para la puesta en marcha de un servicio Web, ambos sistemas operativos cuentan con una aplicación que lleva el nombre de Internet Information Services (Servicios de Información para Internet) o IIS como se le conoce comúnmente. Actualmente IIS se encuentra en la versión 5.0, la cual contiene las siguientes características importantes:

- La flexibilidad y riqueza del lenguaje VBScript es uno de los aspectos más valorados en la arquitectura del IIS y NT. VBSscript permite crear sofisticados comportamientos en la interfaz del usuario (que es el visualizador), realizar esto en Javascript o Perl, por ejemplo, es más difícil y laborioso de mantener.
- La integración con diversos lenguajes de programación, que permite realizar sitios sofisticados o simples páginas Web. Entre los lenguajes mas comúnmente utilizados se encuentran los siguientes:

Lenguaje de Marcas de Hipertexto (HTML). Es bajo el cual operan en esencia las Páginas Web. Hipertexto Significa que existen palabras seleccionadas en un documento, que establecen ligas a otros documentos que pueden estar ubicados en distintos servidores del mundo.

Lenguaje de Marcas de Hipertexto Dinámico (DHTML). No es una tecnología específica, como JavaScript, VBScript o ActiveX, no es una etiqueta, un plug-in o un browser; es más

bien la reunión de diversas tecnologías, JavaScript, VBScript, DOM (Document Object Model: Modelo de Objetos de Documento), Layers (Secciones), CSS (Cascading Style Sheets: Hojas de Estilo en Cascada), con la finalidad de crear páginas que cambian en un visualizador.

Lenguaje de etiquetas expandible (XML). Es un lenguaje surgido a partir de HTML, mientras que este se preocupa por el aspecto de los datos, XML se preocupa por su significado, ya que podemos crear etiquetas propias que describan con precisión lo que deseamos saber. Para procesar los documentos XLS es necesario utilizar un parser o procesador de XML, el cual se instala sobre la plataforma de IIS de forma transparente.

Lenguaje de Marcas de Hipertexto Extendido (XHTML). Se puede decir sin lugar a dudas, que el XHTML está interrelacionado con el XML y HTML, tomando lo mejor de cada uno, como las conocidas y extendidas etiquetas del HTML y la estricta normativa del XML.

Hojas de estilo en cascada (CSS). Es un conjunto de procedimientos que controla distintos aspectos visuales y dinámicos de las páginas Web, tales como fuentes, colores, márgenes y otros. Se constituye con un pequeño archivo que se vincula a una o más páginas, con el cual se consigue un aspecto similar para todas.

Páginas Activas en el Servidor (ASP). Es una tecnología Web que permite crear páginas Web plenamente dinámicas e interactivas con el usuario.

Capítulo 1

SISTEMAS DE IDENTIFICACIÓN

Los sistemas que habitualmente utilizamos los humanos para identificar a una persona, como el aspecto físico o la forma de hablar, son demasiado complejos para una computadora; el objetivo de los sistemas de identificación de usuarios no suele ser identificar a una persona, sino autenticar que esa persona es quien dice ser realmente. Aunque como humanos seguramente ambos términos nos parecerán equivalentes, para una computadora existe una gran diferencia entre ellos: imaginemos un potencial sistema de identificación estrictamente hablando, por ejemplo uno biométrico basado en el reconocimiento de la retina; una persona miraría a través del dispositivo lector y el sistema sería capaz de decidir si es un usuario válido, en ese caso decir de quién se trata; esto es identificación. Sin embargo, lo que habitualmente hace el usuario es introducir su identidad (un número, un nombre de usuario, etc.) además de mostrar sus retinas ante el lector; el sistema en este caso no tiene que identificar a esa persona, sino autenticarlo, comprobar los parámetros de la retina que está leyendo con los guardados en una base de datos para el usuario que la persona dice ser; estamos reduciendo el problema de una población potencialmente muy elevada a un grupo de usuarios más reducido, el grupo de usuarios del sistema que necesita autenticar.

En forma esquemática, la Figura 1.1 muestra los módulos para un sistema de identificación:

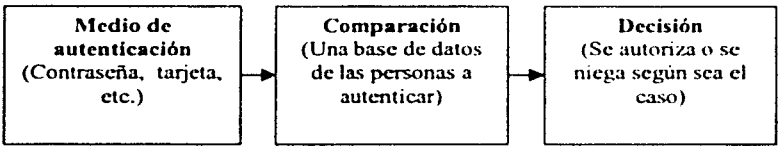


Figura 1.1
Módulos para un sistema de identificación

Los métodos de autenticación pueden pertenecer a diferentes categorías, por ejemplo:

- Algo que el usuario sabe.
- Algo que éste posee.
- Una característica física del usuario o un acto voluntario del mismo.

Esta última categoría se conoce con el nombre de autenticación biométrica. Es fácil ver ejemplos de cada uno de estos tipos de autenticación: una contraseña, es algo que el usuario conoce y el resto de personas no; una tarjeta de identidad, es algo que el usuario lleva consigo; la huella dactilar, es una característica física del usuario y un acto voluntario podría considerarse que se produce al firmar. Por supuesto, un sistema de autenticación puede (y debe, para incrementar su fiabilidad) combinar mecanismos de diferente tipo, como en el caso de una tarjeta de crédito junto al PIN (Número de Identificación Personal, PIN por sus siglas en inglés) a la hora de utilizar un cajero automático.

Cualquier sistema de identificación (aunque les llamemos así, recordemos que realmente son sistemas de autenticación) ha de poseer unas determinadas características para ser

viable; obviamente, ha de ser fiable con una probabilidad muy elevada (podemos hablar de tasas de falla de 10^{-4} en los sistemas menos seguros) y económicamente factible para la organización. Aparte de estas características tenemos otra, no técnica sino humana, pero quizás la más importante: Un sistema de autenticación ha de ser aceptable para los usuarios, que serán al fin y al cabo quienes lo utilicen. Por ejemplo, imaginemos hipotéticamente, un potencial sistema de identificación para acceder a los recursos de una Universidad, consistente en un dispositivo que fuera capaz de realizar un análisis de sangre a un usuario y así comprobar que es quien dice ser; seguramente sería barato y altamente fiable, pero nadie aceptaría dar un poco de sangre cada vez que desee consultar su correo.

1.1 Claves y contraseñas

El modelo de autenticación más básico consiste en decidir si un usuario es quien dice ser, simplemente basándonos en una prueba de conocimiento que *a priori* sólo ese usuario puede superar; desde Alí Babá y su "Ábrete, Sésamo" hasta los más modernos sistemas computacionales, esa prueba de conocimiento no es más que una contraseña que en principio es secreta. Evidentemente, esta aproximación es la más vulnerable a todo tipo de olvidos, pero también la más barata, por lo que se convierte en la técnica más utilizada en entornos que no precisan de un alto control. Otros entornos en los que se suele aplicar este modelo de autenticación son las aplicaciones que requieren de alguna identificación de usuarios. También se utiliza como complemento a otros mecanismos de autenticación, por ejemplo en el caso del Número de Identificación Personal (PIN) a la hora de utilizar cajeros automáticos.

En todos los esquemas de autenticación basados en contraseñas se cumple el mismo protocolo: las entidades (generalmente dos) que participan en la autenticación acuerdan una clave, la cuál se debe de mantener en secreto si desean que la autenticación sea fiable. Cuando una de las partes desea autenticarse ante otra se limita a mostrarle su conocimiento de esa clave común, si ésta es correcta se otorga el acceso a un recurso. Lo habitual es que existan roles preestablecidos, con una entidad activa que desea autenticarse y otra pasiva que admite o rechaza a la anterior.

Para los sistemas de control de acceso, uno de los dispositivos de identificación más utilizado es el basado en contraseñas, el cual, dependiendo de la aplicación que se le quiera dar tendrá su variante. Funcionan de manera similar a las protecciones físicas, las personas que requieran acceder a las instalaciones deben contar con una contraseña que tomará el lugar de una llave, esta deberá ser proporcionada en el punto de acceso y el sistema la validará si cuenta con la autorización correspondiente para ese punto de control.

En este tipo de identificación se utiliza un teclado (*keypad*), que requiere de una secuencia correcta de números en un conjunto de botones para abrir la puerta. En este tipo de identificación tenemos dos modalidades: El sistema del control de acceso más económico es el autónomo, cuyo microprocesador está ubicado en la puerta, este tipo de unidad contiene una memoria EEPROM, donde se encuentran almacenados todos los códigos, su

característica principal es que las claves de acceso son independientes entre cada punto de control (Figura 1.2).

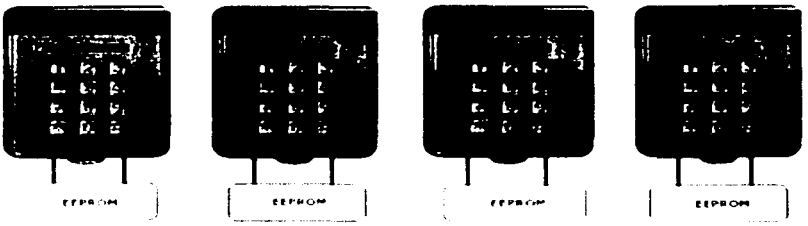


Figura 1.2
Sistema del control con memoria EEPROM

Otro sistema de control de acceso más sofisticado es el que enlaza varias puertas a una computadora central, donde se encuentran almacenadas todas las contraseñas para todos los puntos de control existentes, en este caso, cada vez que una persona ingresa su contraseña, esta es validada y dependiendo de la información proporcionada y la contenida en la base de datos, se otorga o no el acceso (Figura 1.3).

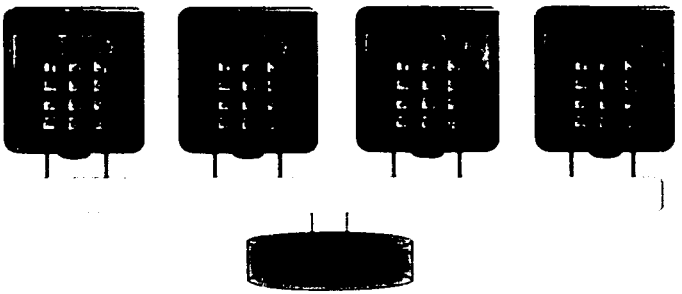


Figura 1.3
Sistema de control con enlace a una computadora central

Como hemos dicho, este esquema es muy frágil basta con que una de las partes no mantenga la contraseña en secreto para que toda la confiabilidad del modelo se pierda; por ejemplo, si el usuario de una máquina comparte su clave con un tercero, o si ese tercero consigue leerla y rompe su cifrado, automáticamente esa persona puede autenticarse ante el sistema con éxito con la identidad de un usuario que no le corresponde.

1.2 Código de Barras

El código de barras es la tecnología de identificación automática predominantemente usada para recoger datos acerca de una persona, lugar u objeto. Sus aplicaciones parecieran ser infinitas. Se utiliza para localización de productos, control de inventario, tiempo y asistencia, monitoreo de trabajo en vía de procesamiento, control de calidad, control de entrada y salida, entrada de órdenes, seguimiento de documentación, control de accesos, identificación personal, envío y recibo de mercancía, almacenamiento, operaciones de punto de venta y en aplicaciones de la industria de la salud, hasta seguimiento del uso de medicamentos al paciente. El código de barras no es un sistema en sí mismo, fundamentalmente, es una herramienta de identificación efectiva que provee datos en tiempo real, los cuales soportan sofisticados sistemas.

1.2.1 Historia

En Octubre de 1949 se patentó el primer sistema de código de barras por Norman Woodland y Bernard Silver. Se trataba de un "tiro al blanco" hecho mediante una serie de círculos concéntricos y se usaba en una banda transportadora de productos para ser leídos por un fotodetector. En 1961 aparece el primer escáner fijo de códigos de barras instalado por Sylvania General Telephone. Este aparato leía barras de colores rojo, azul, blanco y negro identificando vagones de ferrocarriles. Para 1967 la Asociación de Ferrocarriles de Norteamérica en Estados Unidos, aplica códigos de barras para control de tránsito de embarques. El proyecto no duró mucho por falta de adecuado mantenimiento de las etiquetas que contenían el código. En ese mismo año, la cadena de supermercados Kroger en su sucursal de Cincinnati, instala el primer sistema de venta por menudeo basado en código de barras. Al cliente que encontraba un código que no se podía leer correctamente se le ofrecían cupones de compra gratis. En 1969, el láser hace su aparición y usando luz de gas de Helio-Neón, se instala el primer escáner fijo de láser con un costo de $10,000 USD.

En 1969, Rust Oleum fue el primero en interactuar un lector de códigos con una computadora. El programa ejecutaba funciones de mantenimiento de inventarios e impresión de reportes de embarque.

En 1970 aparece la primera terminal portátil de datos fabricado por Norand. Este utilizaba un lápiz de contacto.

El código Plessey hace su aparición en Inglaterra en 1971 en The Plessey Company, para control de archivos en organismos militares. Su aplicación se difundió para control de documentos en bibliotecas. Codabar aparece en ese mismo año y encuentra su mayor aplicación en los bancos de sangre donde se necesita un medio de identificación y verificación automática. Buick, la fábrica de automóviles, utilizó identificación automática en las operaciones de ensamble de transmisiones. El sistema era utilizado para conteo de los diferentes tipos de transmisión de ensamblados diariamente.

El código ITF (Interleaved Two of Five) marca su aparición en 1972, creado por el Dr. David Allais, en ese entonces de Intermec.

En el año 1973 se anuncia el código UPC (Universal Product Code) que se convertiría en el estándar de identificación de productos. De esta forma la actualización automática de inventarios permitía una mejor y más oportuna compra y reabastecimiento de bienes. Europa se hace presente con su propia versión de UPC. En 1976, el código EAN (European Article Number).

En 1974, nuevamente el Dr. Allais, creador del código ITF, conjuntamente con Ray Stevens de Intermec inventan el código 39, el primero de tipo alfanumérico.

El primer sistema patentado de verificación de códigos de barras por medio de laser aparece en el mercado en 1978.

El PostNet, aparece en 1980, siendo usado por el Servicio Postal de los Estados Unidos.

En 1981 surge la tecnología de CCD (Charge Coupled Device) y es aplicada en un escáner. En la actualidad este tipo de tecnología tiene bastante difusión en el mercado asiático, mientras que el láser domina en el mundo occidental. En ese año también aparece el código 128, de tipo alfanumérico.

1.2.2 Funcionamiento

Los códigos de barras trabajan de la siguiente forma, cada carácter es representado por un modelo de barras anchas y estrechas. El programa de lectura utiliza un fotosensor para convertir el código de barras en una señal eléctrica mientras que se mueve a través de él.

El lector después mide las anchuras relativas de las barras y de los espacios, traduce los diversos modelos nuevamente dentro de caracteres regulares y los envía a un decodificador.

Cada código de barras contiene un carácter especial de inicio y de fin. Esto permite al lector determinar si esta leyendo el inicio o el fin del código de barras

Algunos códigos de barras pueden incluir un carácter de suma de comprobación antes del carácter de fin de código. Este carácter se calcula al momento de imprimir el código usando los demás caracteres. El programa de lectura realiza el mismo cálculo y compara su respuesta con el carácter de la suma de comprobación que leyó al final de código de barras. Si no coinciden, el programa de lectura asume que algo es incorrecto y pide realizar otra lectura.

El sistema de codificación que define los datos representados por las barras y espacios es llamado **simbología**. Las más comúnmente usadas son aquellas mencionadas más adelante.

1.2.3 Tipos de Simbología

Hay diversos tipos de simbologías en la actualidad para los códigos de barras. Algunos ya muy viejos y otros que apenas empiezan a abrirse camino mundialmente. Cada uno tiene sus propias características, como por ejemplo el código UPC es todo numérico o el código 39 que incluye letras mayúsculas, dígitos y algunos símbolos.

Código Plessey

Figura 1.4
Ejemplo del código Plessey

El Código Plessey fue desarrollado en Inglaterra y dio origen a varios más, incluyendo los códigos de MSI de Anker y de Telxon. De éstos, el MSI Plessey sigue siendo uno de los códigos más usados en la Unión Americana. Se utiliza en bibliotecas y a menudo para la venta al menudeo de pequeñas tiendas de comestibles.

En el Código MSI Plessey, cada carácter es representado por 4 barras, una barra estrecha representa un 0 binario y una barra ancha representa un 1 binario (Figura 1.4). Las barras tienen los pesos binarios 8-4-2-1. Es posible codificar los dígitos 0 a 9 y las letras A a la F, aunque este código se utiliza más para la información numérica. El carácter de inicio es una sola barra ancha, y el carácter de fin son dos barras estrechas.

La Suma de comprobación del Módulo 10

Un Código MSI Plessey incluye siempre una suma de comprobación del módulo 10 y puede incluir una segunda suma de comprobación. El método para calcular la suma de comprobación es un dígito binario inusual y se calcula de la siguiente forma

- Paso 1. Se forma un nuevo número usando cada dígito del número original. Si la cantidad de dígitos en el número original es par, se comienza con el segundo dígito; si es un número impar, se comienza con el primero. Por ejemplo, si el número original es 123456, el nuevo número será 246; si el número original es 12345, el nuevo número será 135. El último dígito en el nuevo número será siempre el último dígito en el número original.

- Paso 2. Multiplique el nuevo número por 2. Para este caso, el numero original es **12345** y el nuevo número será **135**, por lo tanto 135 x 2 = 270

- Sume entre sí el resultado. En este caso, 2 + 7 + 0 = 9.

- Agregue a este resultado todos los números de la cifra original, sin utilizar los números del paso 2. En nuestro ejemplo son el 2 y el 4.
  9 + 2 + 4 = 15.

- Realice una división del módulo 10 en el resultado y reste el número obtenido. Si el resultado es 10, cámbielo a 0. Usando nuestro ejemplo 10 - (15 modulo 10) = 5. Esta es la suma de comprobación.

- Si se requiere una segunda suma de comprobación, añada la primera suma al final del número original y realice el cálculo de nuevo incluyendo la primera suma de comprobación. En nuestro ejemplo, la suma de comprobación para 12345 sería 5. La segunda suma de comprobación sería calculada usando 123455 como la cadena original.

PostNet (También conocido como 3 de 5)

Figura 1.5
Ejemplo del código PostNet

El código PostNet (Figura 1.5) es utilizado por el servicio postal de los Estados Unidos para clasificar automáticamente el correo. El código PostNet consiste en barras uniformemente espaciadas de dos diversas alturas. Cada carácter es representado por cinco barras, dos altos y tres cortos. El juego de caracteres incluye los dígitos del 0 al 9. El código comienza y termina con una barra alta (barra del marco) y puede contener un código postal de 5 dígitos, un código de 9, o un código de 11 números. Un dígito de suma de comprobación del modulo 10 se inserta después del código postal y antes de la barra del marco de conclusión.

Código 39 (3 DE 9)

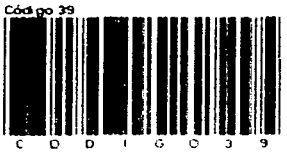


Figura 1.6
Ejemplo del código 39

El código 39 (Figura 1.6) se utiliza extensamente en muchas industrias y es el estándar para muchas especificaciones de código del gobierno de los Estados Unidos incluyendo al departamento de la Defensa. El código 39 se define en el Instituto Nacional Americano de Estándares (ANSI, por sus siglas en inglés) y también se le conoce como USD-3 y 3 de 9.

El juego de caracteres del código 39 incluye los dígitos 0-9, las letras A-Z (mayúsculas solamente) y los símbolos siguientes: espacio, menos (-), más (+), punto (.), signo de dólar ($), diagonal (/) y un carácter especial de inicio/fin. El código puede estar en cualquier longitud, aunque más de 25 caracteres realmente comienza a dificultar su lectura.

Cada carácter consiste en 9 elementos: 5 barras y 4 espacios. Cada carácter incluye 3 elementos anchos y 6 estrechos. Los caracteres son separados por un espacio de la misma anchura que una barra estrecha.

El código 39 no requiere una suma de comprobación, aunque puede llevar un dígito de suma de comprobación del módulo 43 que se puede añadir al final del código para la integridad creciente de los datos (la suma de comprobación del módulo 43 se utiliza raramente). El código 39 es el único tipo de código de uso común que no requiere una suma de comprobación. Esto lo hace especialmente atractivo para las aplicaciones donde es incómodo, difícil o imposible realizar cálculos cada vez que se imprime un código de barras.

Código Extendido 39

El código extendido 39 fue desarrollado para proporcionar un medio para codificar los caracteres adicionales que no forman parte del código 39 (por ejemplo las letras minúsculas y los símbolos). Los caracteres extendidos son codificados por un par de caracteres normales del código 39; por ejemplo, la letra "a" minúscula se puede codificar "+A".

PDF-417

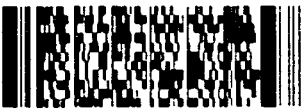


Figura 1.7
Ejemplo del código PDF-417

El PDF-417 (Figura 1.7) es un código de dos dimensiones que puede almacenar cerca de 1800 caracteres imprimibles del código ASCII o 1100 caracteres binarios por etiqueta

Es posible dividir grandes cantidades de datos en varios símbolos PDF-417 que se conecten lógicamente. No hay límite teórico en la cantidad de datos que se puedan salvar en un grupo de los símbolos PDF-417.

La capacidad de PDF-417 puede ser utilizada en las aplicaciones donde la información no está siempre disponible en una base de datos para una búsqueda rápida. El PDF-417 se está utilizando para el etiquetado de materiales peligrosos; guardar especificaciones y datos técnicos de la calibración en los instrumentos electrónicos; huellas digitales y fotografías de codificación en la parte posterior de las licencias en algunos países.

La capacidad máxima de datos es determinada por los elementos más pequeños que pueden ser impresos y explorados confiablemente. Usando la medida recomendada más pequeña de la etiqueta de 0,0075 pulgadas de ancho y 0,010, la capacidad máxima de datos en el modo binario es 686 octetos por pulgada cuadrada (106,2 octetos por centímetro cuadrado). En el modo imprimible del ASCII la densidad es 1.144 caracteres por pulgada cuadrada (177,2 caracteres por centímetro cuadrado).

Las etiquetas PDF-417 requieren de un lector en dos dimensiones o estándar o de láser y software especial de decodificación lógica.

Codabar (También conocido como USD-4, NW-7, y 2 del código 7)

Figura 1.8
Ejemplo del código Codabar

Codabar (Figura 1.8) contiene los dígitos del 0 al 9, seis símbolos (-:.$/+), y los caracteres de inicio/fin A, B, C, D, E, *, N, o T. Los caracteres de inicio/fin se deben utilizar en pares y pueden no aparecer en otra parte del código. Codabar se utiliza en bibliotecas, bancos de sangre y en una gran variedad de aplicaciones.

No existe suma de comprobación definida como parte del estándar de Codabar, pero algunas industrias, sobre todo bibliotecas, han adoptado sus propios estándares de la suma de comprobación. Muchas bibliotecas utilizan el siguiente sistema que incluye 13 dígitos más una suma de comprobación; en la Figura 1.9 se muestra una etiqueta de código de barras para Codabar con el método usado por la Ameritech Library (Provo, Utah).

Figura 1.9
Ejemplo del código Codabar usado por la Ameritech Library (Provo, Utah)

- El dígito 1 indica el tipo de código: 2 = patrón, 3 = artículo (en este caso un libro).
- Los dígitos 2-5 identifican a la institución (3191).
- Los 9 dígitos siguientes (00010 586) identifican el patrón o el artículo individual (título, por ejemplo).
- El dígito 14 es la suma de comprobación.

Para calcular la suma de comprobación, se comienza con el conjunto total a cero y explore los 13 dígitos de izquierda a derecha:

- Si el dígito está en una posición con número par (2, 4, 6...) agréguela al total.
- Si el dígito está en una posición con números impares (1, 3, 5...) multiplique el dígito por 2. Si el producto es igual a o mayor de 10, reste 9. Entonces agregue el producto al total.
- Después de que se hayan procesado todos los dígitos, divida el total por 10 y tome el resto.
- Si el resto es = 0, es que ese es el dígito de la suma de comprobación. Si el resto no es cero, el dígito de la suma de comprobación es 10 menos el resto.

Por ejemplo para este caso nuestro número es:

3 3 1 9 1 0 0 0 1 0 5 8 6 4

- Colocando los números por posición:

3
3
1
9
1
0
0
0
1
0
5
8
6

- Tomando los números de posición par y haciendo la suma:

$$3 + 9 + 0 + 0 + 0 + 8 = 20$$

- Tomando los números con posición impar:

$$3 \times 2 = 6$$
$$1 \times 2 = 2$$
$$1 \times 2 = 2$$
$$0 \times 2 = 0$$
$$1 \times 2 = 2$$
$$5 \times 2 = 10 \text{ número igual a 10 se resta 9,}$$
$$6 \times 2 = 12 \text{ número mayor a 10 se resta 9}$$

- Por lo tanto la suma de números con posición impar queda así:

$$6 + 2 + 2 + 0 + 2 + 1 + 3 = 16$$

- haciendo la suma total:

$$16 + 20 = 36$$

- Dividiendo por 10:

$$36/10 = 3\frac{6}{10}$$

- como el resultado es $\neq 0$ entonces restamos:

$$10 - 6 = 4$$

El resultado coincide con el dígito número 14, por lo tanto la comprobación es correcta.

UPC-A

Figura 1.10
Ejemplo del código UPC-A

El código UPC-A (Figura 1.10) se utiliza para marcar productos que se ponen a la venta al menudeo en los Estados Unidos. El código identifica el fabricante y al producto al momento de la compra y automáticamente coloca el precio en la pantalla.

UPC-E

Figura 1.11
Ejemplo del código UPC-E

UPC-E (Figura 1.11) es una variación del símbolo de UPC-A que se utiliza para el sistema de numeración 0. Suprimiendo ceros, los códigos de UPC-E se pueden imprimir en un espacio muy pequeño y se utilizan para etiquetar artículos pequeños.

Además del requisito que el primer dígito del código (sistema de numeración) debe ser cero, hay cuatro reglas que determinan qué códigos del UPC se pueden imprimir usando el formato comprimido de UPC-E:

- Si los 3 últimos dígitos de un número de fabricante son 000, 100, ó 200, los números de código válidos de producto son 00000 - 00999 (1.000 números).
- Si los 3 últimos dígitos del número del fabricante son 300, 400, 500, 600, 700, 800, ó 900, los números de código válidos de producto son 00000 - 00099 (100 números).
- Si los 2 últimos dígitos del número del fabricante son 10, 20, 30, 40, 50, 60, 70, 80, ó 90, los números de código válidos de producto son 00000 - 00009 (10 números).

- Si el número del fabricante no termina en cero, los números de código válidos de producto son 00005 - 00009 (5 números).

EAN-13

Figura 1.12
Ejemplo del código EAN-13

EAN-13 (Figura 1.12) se utiliza en todo el mundo para la venta de mercancías al menudeo. El símbolo codifica 13 caracteres: los primeros dos o tres son un código que identifican al país en el cual se encuentra el fabricante (no necesariamente donde el producto se hace originalmente). El código de país es seguido por 9 ó 10 dígitos de los datos (dependiendo de la longitud del código de país) y uno solo de la suma de comprobación.

La suma de comprobación es un cálculo del módulo 10:

- Sume los valores de los dígitos en las posiciones numeradas por pares: 2, 4, 6, etc.
- Multiplique este resultado por 3.
- Agregue los valores de los dígitos en las posiciones con números impares: 1, 3, 5, etc.
- Sume los resultados de los pasos de progresión 2 y 3.
- El carácter de la suma de comprobación es el número más pequeño que, cuando está agregado al resultado en el paso de progresión 4, produce un múltiplo de 10.

Ejemplo: Asuma los datos del código = **001234567890**

- 0 + 2 + 4 + 6 + 8 + 0 = 20
- 20 * 3 = 60
- 0 + 1 + 3 + 5 + 7 + 9 = 25
- 60 + 25 = 85
- 85 + X = 90 **(el múltiplo igual o más alto más cercano de 10), por lo tanto X = 5 (suma de comprobación)**

EAN-8

Figura 1.13
Ejemplo del código EAN-8

EAN-8 (Figura 1.13) es una versión acortada del código EAN-13. Incluye un código de país de 2 ó 3 dígitos, 4 ó 5 dígitos de los datos (dependiendo de la longitud del código de país), y un dígito de la suma de comprobación. Mientras que es posible agregar el código de una extensión de 2 dígitos ó 5 dígitos, el propósito primario del código EAN-8 es utilizar tan poco espacio como sea posible.

Semejante al código de UPC-E, que comprime los datos que se podrían imprimir como código del mismo tamaño de UPC-A, los dígitos de los datos en un símbolo EAN-8 identifican específicamente un producto y un fabricante determinados. Puesto que un número limitado de los códigos EAN-8 está disponible en cada país, se publican solamente para los productos con el espacio determinado para un símbolo normal EAN-13. Por ejemplo, un código de país de 2 dígitos permite un total de solamente 100,000 números de productos.

CÓDIGO 128

Figura 1.14
Ejemplo del código 128

El Código 128 (Figura 1.14) proporciona la cantidad adecuada para un gran tamaño de datos alfanuméricos. Se selecciona a menudo en nuevas aplicaciones, debido a su capacidad y porque ofrece una selección mucho más grande de caracteres.

El juego de caracteres del Código 128 incluye los dígitos 0-9, las letras A-Z (mayúsculas y minúsculas) y todos los símbolos del código ASCII y códigos de control estándares. Los códigos se dividen en tres subconjuntos A, B, y C. Hay tres códigos separados del comienzo para indicar qué subconjunto será utilizado; además, cada subconjunto incluye caracteres de control para cambiar a otro subconjunto en el centro de un código. El subconjunto A incluye los símbolos estándares del ASCII, los dígitos, las letras mayúsculas, y los códigos de control. El subconjunto B incluye letras estándares de los símbolos, de los dígitos, mayúsculas y minúsculas del ASCII. El subconjunto C comprime dos dígitos numéricos en cada carácter.

1.2.4 Características de la simbología

En la Tabla 2 se resumen las diferentes características de la simbología de varios códigos de barras:

Simbología	Longitud	Checksum*	Caracteres**	Notas:
Code 39	2-30	NR	N,U,P	Código de barras más común
Code 128	2-30	Auto	N,U,L,P,C	Mejor debido a conjunto total de caracteres ASCII
UPC-A	11,13,16	Auto	N	Estándar para abarrotes
UPC-E	11,13,16	Auto	N	Empaques pequeños
EAN/JAN-13	12,14,17	Auto	N	UPC + código del país
EAN/JAN-8	7,9,12	Auto	N	UPC + código del país
Extended 39	2-30	NR	N,U,L,P,C	Casilla inferior/Ctrl-muy ancho
Codabar	2-30	NR	N	Requiere inicio/fin (A,B,C, o D)
PostNet	5,9,11	Auto	N	Posiciones críticas
***Checksum** **Auto**=checksum automático-siempre requerido **NR**=Checksum no requerido-auto revisión **Recmd**= Checksum ampliamente recomendado				****Caracteres codificados** **N** Números (0-9) - casilla superior (A-Z) **L**=Casilla inferior (a-z) **P**=Puntuación **C**=Caracteres de control (< 32)

Tabla 2
Resumen de características de la simbología de los códigos de barras

1.3 Tecnología de tarjetas

Las tarjetas de banda magnética y de proximidad son las más comúnmente usadas hoy en día. Las tarjetas de proximidad son de "manos-libres". Estas tarjetas no tienen que insertarse en la lectora, sino que ésta las reconoce cuando están cerca (a pocos centímetros). Mientras la aceptación general de las tarjetas de proximidad va en aumento, el tipo más común de tarjeta de control de acceso es el de banda magnética

1.3.1 Tarjetas magnéticas

Son tarjetas plásticas con una banda de color oscuro en la parte posterior llamada banda magnética.

Debido a su amplio uso, la mayoría de las tarjetas se adhieren a estándares bien definidos que describen sus características físicas y magnéticas. Estos estándares sugieren especificaciones para almacenamiento e intercambio de datos, pero no evitan que se utilicen técnicas diferentes para aplicaciones específicas.

Según la norma ISO 2894 las tarjetas magnéticas se fabrican con material PVC especial y cuentan con las siguientes medidas (Figura 1.15):

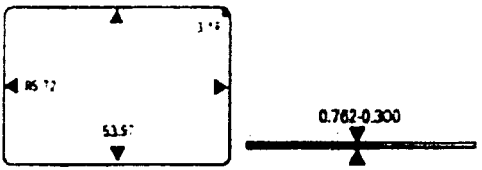


Figura 1.15
Medidas de las tarjetas magnéticas

En la Figura 1.16, se muestra de qué está compuesta la tarjeta internamente.

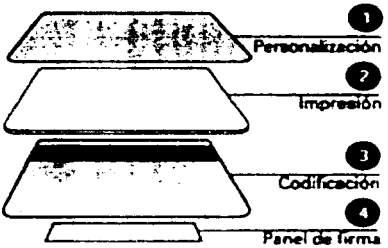


Figura 1.16
Composición de las tarjetas magnéticas

La capa de personalización de las tarjetas incluye el estampado, imágenes digitalizadas, etc., en la segunda capa se imprime el diseño de la entidad emisora, en la tercera capa se incluye la codificación de la tarjeta mediante banda magnética y/o código de barras, y en la última capa (panel de firma) se incluye un panel de textura especial, que permite la escritura o la firma del titular.

La banda magnética (banda oscura) contiene la información correspondiente que la hace única cuando le pertenece a un individuo, esta banda a su vez está compuesta por tres bandas de datos diferentes (Figura 1.17), cada banda tiene su propio formato de codificación definida.

La banda más utilizada es de un ancho de 1/2 pulgada. La capacidad de grabación de la banda varia en función de la pista.

- Pista 1: 210 bits por pulgada y acepta 79 caracteres alfanuméricos útiles.
- Pista 2: 75 bits por pulgada y acepta 40 caracteres numéricos útiles.
- Pista 3: 210 bits por pulgada y acepta 107 caracteres numéricos útiles.

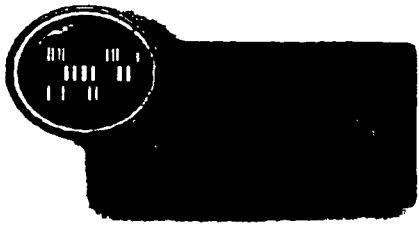


Figura 1.17
Composición de la banda magnética

Las bandas magnéticas están hechas de un pigmento a base de pequeñas partículas ferromagnéticas (esto quiere decir que, al someterlas a un campo magnético, se convierten en pequeños imanes permanentes) embebidas en una matriz de resina. En el momento de la grabación, un solenoide o electroimán va pasando a lo largo de la banda, dependiendo del sentido en que circule la corriente eléctrica por el solenoide éste inducirá una polaridad u otra a las partículas ferromagnéticas, de esta forma cuando la banda ha sido grabada, tendremos en ella una fila de zonas en las que las partículas estarán magnetizadas en la misma dirección.

Las bandas magnéticas se clasifican por su grado de resistencia a los campos magnéticos (coercitividad) en bandas de baja y alta:

- LO-CO: Banda magnética de baja densidad, habitual en las tarjetas de uso bancario, requiere una coercitividad de 300 Oersted. Muy apta para empresas provistas de lectores-grabadores.

- HI-CO: Banda magnética de alta densidad (desde 2540 hasta 4000 Oersted). De gran resistencia a campos magnéticos, y una vez grabada es practicamente imposible su descodificación.

La lectura se realizara con un solenoide (estos solenoides son lo que llamamos normalmente cabezales), cuando deslizamos una tarjeta por el cabezal lector, éste produce una señal eléctrica que algún aparato (caja registradora, microcontrolador, computadora personal...) tendrá que decodificar. Esta señal suele comenzar con una fila de ceros que

sirve para sincronizar el lector con los bits de la pista, a continuación vienen los datos y por último, la pista se acaba con una fila de bits "de relleno" que pueden ser unos o ceros.

Existen a su vez en el mercado lectoras con señal no decodificada, o bien con salida decodificada ya sea por RS232 con estrada al puerto serial o bien como emuladoras de teclado.

Para este tipo de tarjetas es importante tener algunos cuidados, ya que cuando tarjetas ralladas o gastadas se introducen en el lector, las partículas férricas se clavan en la cerámica del cabezal lector, estas partículas no desaparecen totalmente con la limpieza del cabezal, y contribuyen a rallar las demás tarjetas que se introduzcan, desgastando prematuramente el cabezal y acortando su vida útil. Cuando se introducen tarjetas sucias en el lector, esta suciedad se adhiere al cabezal lector y aumenta la distancia de lectura entre la banda magnética de la tarjeta y el cabezal, dificultando las lecturas posteriores.

La aplicación más conocida de banda magnética la tenemos en las tarjetas de crédito y débito que se utilizan en los cajeros automáticos y en terminales de punto de venta. La banda magnética también se utiliza para control de accesos en edificios con ingreso restringido, habitaciones de hotel y otras aplicaciones. Otros usos incluyen sistemas de tiempo y asistencia, seguimiento de inventario, identificación personal, parques de diversiones, control de proceso de fabricación, recolección de pagos de tránsito, etc. La tecnología de banda magnética permite el almacenamiento de una moderada cantidad de datos en un área pequeña. Una sola banda magnética puede tener varias vías de información grabadas. A diferencia de otras formas de almacenamiento de datos, la información contenida en una tarjeta con banda magnética puede ser reesenta y actualizada. Una aplicación que está ganando terreno rapidamente es el uso de la tarjeta de banda magnética para autorizar y liberar beneficios del gobierno, tales como fondos, estampillas para compra de alimentos y servicios. Otra aplicación en vías de gran crecimiento son las tarjetas con valor almacenado. La tarjeta se compra con un valor específico codificado y luego se utiliza para comprar mercancías o servicios. El valor contenido en la tarjeta se reduce magnéticamente, cada vez que se le utiliza. Dos aplicaciones ideales son las tarjetas de llamadas telefónicas y las tarjetas para uso en el peaje de autopistas. Otros usos incluyen programas de comidas para estudiantes, pagos de ingreso a puentes y caminos, video clubes, máquinas expendedoras y licencias de conducir codificadas. Anualmente, se utilizan más de mil millones de tarjetas de banda magnetica en una amplia variedad de aplicaciones.

Actualmente, las tarjetas de banda magnética se ven amenazadas por las tarjetas inteligentes, que cuentan con un microprocesador o chip de memoria incrustado y ofrecen mayores capacidades de almacenamiento; sin embargo, las tarjetas de banda magnética continúan mejorando y se espera que permanezcan en el mercado por mucho tiempo más.

1.3.2 Tarjetas Ópticas

Una tarjeta de memoria óptica es una tarjeta de almacenamiento de datos segura y durable, la cual es leída usando luz proveniente de un láser. Aunque la misma no es más grande que

una tarjeta de crédito, una tarjeta de memoria óptica tiene una capacidad de almacenamiento de información del tamaño de un libro. La capacidad total es de alrededor de 4 Megabytes, lo cual resulta en una capacidad de 2.8 Megabytes para el usuario. Esta capacidad es suficiente para almacenar archivos digitales con miles de páginas de texto o hasta 200 páginas digitalizadas. Estas tarjetas ópticas también conocidas como "escriba una vez, lea muchas veces" (WORM), aseguran que los archivos y datos almacenados en la memoria de la tarjeta están seguros y a salvo de ser violados o borrados o accidentalmente perdidos. Se pueden agregar archivos a las tarjetas o actualizarse pero no borrarse, de la misma manera en que se graba un CD (disco compacto). Cuando se agregan o actualizan archivos, un récord permanente de todos los accesos y cambios efectuados se graba automáticamente en el medio óptico. Y como el mismo es óptico, no es afectado por campos magnéticos o electrostáticos y puede soportar temperaturas de hasta 100°C.

Las tarjetas de memoria óptica son la solución ideal para aquellas aplicaciones que requieren almacenamiento y transporte de datos fuera de línea en un dispositivo de bajo costo, seguro y durable. Las tarjetas de memoria óptica pueden incluir impresión térmica de color, banda magnética, un chip de IC (Circuitos Integrados) y formatos de seguridad. Estos rasgos hacen también que la tarjeta de memoria óptica sea una tarjeta de identificación de alta seguridad.

1.3.3 Tarjetas Inteligentes

Hace más de veinte años un periodista francés llamado Roland Moreno patentaba la integración de un procesador en una tarjeta de plástico; sin duda, no podía imaginar el abanico de aplicaciones de seguridad que ese nuevo dispositivo, denominado tarjetas con chip, estaba abriendo. Desde entonces, cientos de millones de esas tarjetas han sido fabricadas, y son utilizadas a diario para fines que varían desde las tarjetas monedero más sencillas hasta el control de accesos a instalaciones militares y agencias de inteligencia de todo el mundo. Cuando a las tarjetas con chip se les incorporó un procesador inteligente nacieron las tarjetas inteligentes, una gran revolución en el ámbito de la autenticación de usuarios.

Las tarjetas inteligentes usan una tarjeta de plástico del tamaño de una tarjeta de crédito con uno o más microchips incorporados a la misma. Estrictamente hablando, las tarjetas inteligentes son programables, contienen un microprocesador y contienen una gran base de datos. El microprocesador controla la entrada de seguridad a una o más bases de datos de aplicación. Las tarjetas inteligentes tienen normalmente un microprocesador aunque algunas sólo tienen memoria. El término "tarjeta inteligente" tambien se aplica a tarjetas de plástico que sólo tienen memoria y son utilizadas para aplicaciones tales como reemplazo de moneda o unidades de inventario. Estas tarjetas de memoria con circuitos integrados sólo de lectura (IC ROM), también se les conoce como tarjetas de memoria IC, no son programables, pero pueden contener una gran cantidad de datos. Son similares en concepto a las tarjetas de banda magnética, pero los datos estan escondidos y la cantidad de datos almacenados es mayor. Las tarjetas inteligentes y las tarjetas IC pueden tener también

banda magnética que contienen algunos de los datos almacenados en la memoria de la tarjeta inteligente. Esto permite que la tarjeta sea utilizada como una tarjeta plástica común con terminales pre-existentes. Las tarjetas IC que no tienen procesadores son similares en su función a las tarjetas ópticas. Las tarjetas inteligentes son usualmente leídas a través de una superficie de contacto. Las tarjetas inteligentes que no son de contacto se leen en forma remota por señales de radio-frecuencia para aplicaciones de cobro en puestos de ingreso o egreso de puentes y autopistas, identificación de vehículos y contenido de contenedores. La diferenciación entre tarjetas inteligentes sin contacto y ciertos tipos de sistemas de identificación de radio-frecuencia es confusa a veces.

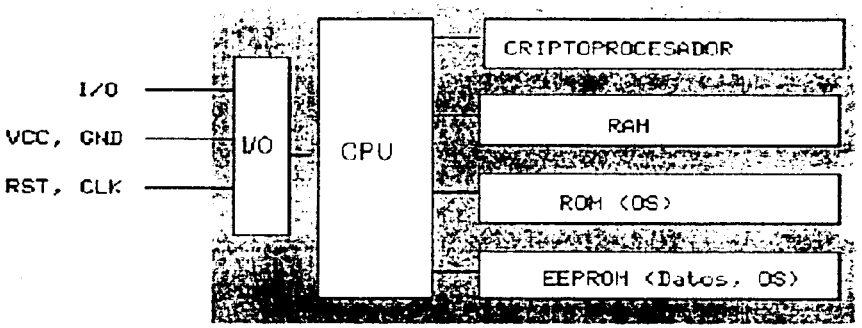


Figura 1.18
Estructura general de una tarjeta inteligente

En la figura 1.18 se muestra la estructura más general de una tarjeta inteligente; en ella podemos observar que el acceso a las áreas de memoria solamente es posible a través de la unidad de entrada - salida y de una CPU (típicamente de 8 bits), lo que evidentemente aumenta la seguridad del dispositivo. Existe también un sistema operativo empotrado en la tarjeta - generalmente en ROM, aunque también se puede extender con funciones en la EEPROM - cuya función es realizar tareas criptográficas (algoritmos de cifrado como RSA o Triple DES); el criptoprocesador apoya estas tareas ofreciendo operaciones RSA con claves de 512 a 1024 bits. Un ejemplo de implementación real de este esquema lo constituye la tarjeta inteligente CERES, de la Fábrica Nacional de Moneda y Timbre española; en ella se incluye además un generador de números aleatorios junto a los mecanismos de protección internos de la tarjeta.

1.4 Sistemas Biométricos

La finalidad de un sistema de control de acceso radica en permitir a las personas que estén autorizadas, a ingresar dentro a un ámbito o lugar específico; esto se puede lograr, gracias a un dispositivo de identificación. Los sistemas bajo los cuales se trabaja usando una

contraseña, requieren que sólo un individuo tenga conocimiento acerca del número clave que se necesitará para ingresar. No se puede identificar si quien posee la contraseña es realmente quien está autorizado. En cambio, los sistemas biométricos, permiten reconocer a la persona por sus características personales como lo es una mano, un ojo, huellas digitales o voz.

La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.

La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y guardado - en un proceso de enrolamiento - dentro de una base de datos. Los lectores biométricos identifican a la persona por lo que es en realidad, a diferencia de la contraseña o claves de acceso.

Independientemente de la técnica que se utilice, el método de operación es siempre la verificación de la identidad de la persona para una comparación de las medidas de determinado atributo físico. Restringido a través de su historia por su costo elevado, una función cuestionable y proveedores transitorios, la identificación biométrica está experimentando ahora una aceptación creciente, no sólo en aplicaciones de alta seguridad tales como bancos e instalaciones gubernamentales, sino también en clubes, la Villa Olímpica en Atlanta en 1996, control de clientes del seguro social y acceso a oficinas y plantas comerciales e industriales. Los costos han estado reduciendo, sin embargo, siguen siendo muy superior a otros sistemas de identificación

1.4.1 Funcionamiento

Los dispositivos biométricos tienen tres partes principales; por un lado, disponen de un mecanismo automático que lee y captura una imagen digital o analógica de la característica a analizar. Además disponen de una entidad para manejar aspectos como la compresión, almacenamiento o comparación de los datos capturados con los guardados en una base de datos (que son considerados válidos), también ofrecen una interfaz para las aplicaciones que los utilizan.

El proceso general de autenticación sigue unos pasos comunes a todos los modelos de autenticación biométrica: captura o lectura de los datos que el usuario a validar presenta, extracción de ciertas características de la muestra (por ejemplo, las minucias de una huella dactilar), comparación de tales características con las guardadas en una base de datos, y decisión de si el usuario es válido o no.

Por último, y antes de entrar más a fondo con los esquemas de autenticación biométrica clásicos, quizás es conveniente desmentir uno de los grandes mitos de estos modelos: la vulnerabilidad a ataques de simulación. En cualquier película o libro de espías que se precie, siempre se consigue "engañar" a sistemas biométricos para conseguir acceso a determinadas instalaciones mediante estos ataques: se simula la parte del cuerpo a analizar mediante un modelo o incluso utilizando órganos amputados a un cadáver o al propio usuario vivo (crudamente, se le corta una mano o un dedo, se le saca un ojo para conseguir

que el sistema permita la entrada). Evidentemente, esto sólo sucede en la ficción: hoy en día cualquier sistema biométrico (con excepción, quizás, de algunos modelos basados en voz) es altamente inmune a estos ataques. Los analizadores de retina, de iris o de huellas son capaces, aparte de decidir si el miembro pertenece al usuario legítimo, de determinar si éste está vivo o se trata de un cadáver.

1.4.2 Reconocimiento de huella digital

Típicamente la huella dactilar de un individuo ha sido un patrón bastante bueno para determinar su identidad de forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona. Por tanto, parece obvio que las huellas se convertirían antes o después en un modelo de autenticación biométrico.

Desde el siglo pasado hasta nuestros días se vienen realizando con éxito clasificaciones sistemáticas de huellas dactilares en entornos policiales, el uso de estos patrones fue uno de los primeros en establecerse como modelo de autenticación biométrica.

Figura 1.19
Huella digitalizada con sus minucias

Cuando un usuario desea autenticarse ante el sistema coloca su dedo en un área determinada (área de lectura, no se necesita en ningún momento una impresión en tinta) Aquí se toma una imagen que posteriormente se normaliza mediante un sistema de finos espejos para corregir ángulos y es de esta imagen normalizada de la que el sistema extrae las minucias (ciertos arcos, bucles o remolinos de la huella) que va a comparar contra las

que tiene en su base de datos; es importante resaltar que lo que el sistema es capaz de analizar no es la huella en sí sino que son estas minucias, concretamente la posición relativa de cada una de ellas.

Está demostrado que dos dedos nunca pueden poseer más de ocho minucias comunes, y cada uno tiene al menos 30 ó 40 de éstas (en la Figura 1.19 podemos ver una imagen de una huella digitalizada con sus minucias). Si la comparación de las posiciones relativas de las minucias leídas con las almacenadas en la base de datos es correcta, se permite el acceso al usuario, negándoselo obviamente en caso contrario.

Los sistemas basados en reconocimiento de huellas son relativamente baratos (en comparación con otros biométricos, como los basados en patrones retinales); sin embargo, tienen en su contra la incapacidad temporal de autenticar usuarios que se hayan podido herir en el dedo a reconocer (un pequeño corte o una quemadura que afecte a varias minucias pueden hacer inútil al sistema). También elementos como la suciedad del dedo, la presión ejercida sobre el lector o el estado de la piel pueden ocasionar lecturas erróneas. Otro factor a tener muy en cuenta contra estos sistemas es psicológico, no técnico: hemos dicho en la introducción que un sistema de autenticación de usuarios ha de ser aceptable por los mismos, y generalmente el reconocimiento de huellas se asocia a los criminales, por lo que muchos usuarios recelan del reconocedor y de su uso.

1.4.3 Reconocimiento de voz

En los sistemas de reconocimiento de voz no se intenta, como mucha gente piensa, reconocer lo que el usuario dice, sino identificar una serie de sonidos y sus características para decidir si el usuario es quien dice ser. Para autenticar a un usuario utilizando un reconocedor de voz se debe disponer de ciertas condiciones para el correcto registro de los datos, como ausencia de ruidos, reverberaciones o ecos; idealmente, estas condiciones han de ser las mismas siempre que se necesite la autenticación

Cuando un usuario desea acceder al sistema pronunciará unas frases en las cuales reside gran parte de la seguridad del protocolo; en algunos modelos, los denominados de texto dependiente, el sistema tiene almacenadas un conjunto muy limitado de frases que es capaz de reconocer: por ejemplo, imaginemos que el usuario se limita a pronunciar su nombre, de forma que el reconocedor lo entienda y lo autentique; estos modelos proporcionan poca confiabilidad en comparación con los de texto independiente, donde el sistema va "proponiendo" a la persona la pronunciación de ciertas palabras extraídas de un conjunto bastante grande. De cualquier forma, sea cual sea el modelo, lo habitual es que las frases o palabras ya establecidas para maximizar la cantidad de datos que se pueden analizar (por ejemplo, frases con una cierta entonación, pronunciación de los diptongos, palabras con muchas vocales). Conforme va hablando el usuario, el sistema registra toda la información que le es útil; cuando termina la frase, ya ha de estar en disposición de facilitar o denegar el acceso, en función de la información analizada y contrastada con la de la base de datos.

El principal problema del reconocimiento de voz es la inmunidad frente a simuladores de voz, un modelo de ataques de simulación en los que un atacante reproduce (por ejemplo,

por medio de un magnetófono) las frases o palabras que el usuario legítimo pronuncia para acceder al sistema. Este problema es especialmente grave en los sistemas que se basan en textos preestablecidos: volviendo al ejemplo anterior, el del nombre de cada usuario, un atacante no tendría más que grabar a una persona que pronuncia su nombre ante el autenticador y luego reproducir ese sonido para conseguir el acceso; casi la única solución consiste en utilizar otro sistema de autenticación junto al reconocimiento de voz. Por el contrario, en modelos de texto independiente, más interactivos, este ataque no es tan sencillo porque la autenticación se produce realmente por una especie de desafío-respuesta entre el usuario y la máquina, de forma que la cantidad de texto grabado habría de ser mucho mayor (y la velocidad para localizar la parte del texto que el sistema propone habría de ser elevada). Otro grave problema de los sistemas basados en reconocimiento de voz es el tiempo que el usuario emplea hablando delante del analizador, al que se añade el que este necesita para extraer la información y contrastarla con la de su base de datos; aunque actualmente en la mayoría de sistemas basta con una sola frase, es habitual que el usuario se vea obligado a repetirla porque el sistema le deniega el acceso (una simple congestión hace variar el tono de voz, aunque sea levemente, y el sistema no es capaz de decidir si el acceso ha de ser autorizado o no; incluso el estado anímico de una persona varía su timbre). A su favor, el reconocimiento de voz posee la cualidad de una excelente acogida entre los usuarios, siempre y cuando su funcionamiento sea correcto y éstos no se vean obligados a repetir lo mismo varias veces, o se les niegue un acceso porque no se les reconoce correctamente.

1.4.4 Geometría de la mano

Uno de los primeros dispositivos biométricos utilizaba la geometría de la mano (Figura 1.20) como tecnología para permitir el acceso a lugares específicos, a este dispositivo se lo llamó IDENTIMAT.

La compañía BioMet Partners es propietaria del sistema Digi-2 el cual fue creado en 1994 y verifica un individuo según el tamaño y la forma de dos dedos, su tiempo de verificación es de 1 segundo y permite el trabajo en red.

La compañía Recognition System Inc. introdujo su primer sistema en 1986, luego de unos años, en 1991, logró reducir el costo de la tecnología lanzando al mercado el sistema de reconocimiento ID3D Hand Key. Este sistema evalúa una imagen tridimensional de los cuatro dedos y parte de la mano para identificar a una persona.

Los sistemas de autenticación basados en el análisis de la geometría de la mano son, sin duda, los más rápidos dentro de los biométricos con una probabilidad de error aceptable en la mayoría de las ocasiones, en aproximadamente un segundo son capaces de determinar si una persona es quien dice ser.

Cuando un usuario necesita ser autenticado coloca su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura. Una vez que la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos (anchura, longitud, área, determinadas distancias) en un formato de

tres dimensiones. Transformando estos datos en un modelo matemático que se contrasta contra una base de patrones, el sistema es capaz de permitir o denegar acceso a cada usuario.

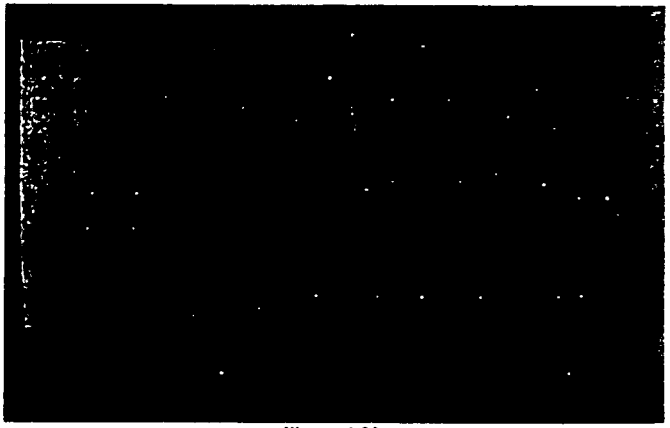


Figura 1.20
Geometría de la mano

Quizás uno de los elementos más importantes del reconocimiento mediante analizadores de geometría de la mano es que éstos son capaces de aprender: a la vez que autentican a un usuario, actualizan su base de datos con los cambios que se puedan producir en la muestra (un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida); de esta forma son capaces de identificar correctamente a un usuario cuya muestra se tomó hace años, pero que ha ido accediendo al sistema con regularidad. Este hecho, junto a su rapidez y su buena aceptación entre los usuarios, hace que los identificadores basados en la geometría de la mano sean los más extendidos dentro de los biométricos a pesar de que su tasa de falsa aceptación se podría considerar inaceptable en algunas situaciones, no es normal, pero sí posible, que dos personas tengan la mano lo suficientemente parecida como para que el sistema las confunda. Para minimizar este problema se recurre a la identificación basada en la geometría de uno o dos dedos, que además puede usar dispositivos lectores más baratos y proporciona incluso más rapidez.

1.4.5 Patrones Oculares

Los modelos de autenticación biométrica basados en patrones oculares se dividen en dos tecnologías diferentes: o bien analizan patrones retinales, o bien analizan el iris. Estos métodos se suelen considerar los más efectivos: para una población de 200 millones de potenciales usuarios la probabilidad de coincidencia es casi 0, y además una vez muerto el

individuo los tejidos oculares degeneran rápidamente, lo que dificulta la falsa aceptación de atacantes que puedan robar este órgano de un cadáver.

La principal desventaja de los métodos basados en el análisis de patrones oculares es su escasa aceptación; el hecho de mirar a través de un binocular (o monocular), necesario en ambos modelos, no es cómodo para los usuarios, ni aceptable para muchos de ellos: por un lado, los usuarios no se fían de un haz de rayos analizando su ojo y por otro un examen de este órgano puede revelar enfermedades o características médicas que a muchas personas les puede interesar mantener en secreto, como el consumo de alcohol o de ciertas drogas. Aunque los fabricantes de dispositivos lectores aseguran que sólo se analiza el ojo para obtener patrones relacionados con la autenticación, y en ningún caso se viola la privacidad de los usuarios, mucha gente no cree esta postura oficial (aparte del hecho de que la información es procesada vía software, lo que facilita introducir modificaciones sobre lo que nos han vendido para que un lector realice otras tareas de forma enmascarada). Por si esto fuera poco, se trata de sistemas demasiado caros para la mayoría de las organizaciones, y el proceso de autenticación no es todo lo rápido que debiera en poblaciones de usuarios elevadas. De esta forma, su uso se ve reducido casi sólo a la identificación en sistemas de alta seguridad, como el control de acceso a instalaciones militares.

Retina

La vasculatura retinal (forma de los vasos sanguíneos de la retina humana) es un elemento característico de cada individuo, por lo que numerosos estudios en el campo de la autenticación de usuarios se basan en el reconocimiento de esta vasculatura.

En los sistemas de autenticación basados en patrones retinales el usuario a identificar ha de mirar a través de unos binoculares, ajustar la distancia interocular y el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis. En ese momento se escanea la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos; Si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.

La compañía EyeDentify posee la patente mundial para analizadores de vasculatura retinal, por lo que es la principal desarrolladora de esta tecnología .

Iris

El segundo sistema de identificación de patrones oculares es aquel que "lee" el iris del ojo, codificando digitalmente, cada una de las imágenes que absorbe.

El órgano protector interno del ojo puede ser reconocido a una distancia de aproximadamente un metro y revelar alrededor de 266 grados de inmunidad de textura del ojo del individuo. Se utiliza menos información, pues con 3 ó 4 bits se obtiene una muestra de la superficie del iris, la cual debe estar contenida en la base de datos. Dicho organo está compuesto por un tejido elástico que completa su desarrollo en el octavo mes de gestación.

Durante el primer año de vida, la corona que compone al ojo cambia de color, y luego permanece en el individuo por el resto de su vida. El uso por parte de un atacante de órganos replicados o simulados para conseguir una falsa aceptación es casi imposible con análisis infrarrojo, capaz de detectar con una alta probabilidad si el iris es natural o no.

La identificación basada en el reconocimiento de iris es más moderna que la basada en patrones retinales; desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios. Para ello, se captura una imagen del iris en blanco y negro, en un entorno correctamente iluminado; esta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas hasta obtener una cantidad de datos (típicamente 256 KBytes) suficiente para los propósitos de autenticación. Esa muestra, denominada iriscode (en la Figura 1.21 se muestra una imagen de un iris humano con su iriscode asociado) es comparada con otra tomada con anterioridad y almacenada en la base de datos del sistema, de forma que si ambas coinciden el usuario se considera autenticado con éxito; la probabilidad de una falsa aceptación es la menor de todos los modelos biométricos.

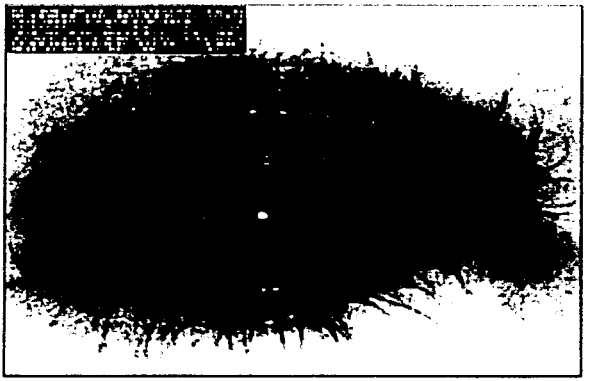


Figura 1.21
Iris humano con su iriscode asociado

La empresa estadounidense IriScan es la principal desarrolladora de esta tecnología (y de investigaciones) basada en reconocimiento de iris que existe actualmente, ya que posee su patente.

El futuro radica en la perfección de cámaras de video de alta resolución. O sea, se trata de eliminar el actual escáner, que funciona con un láser de baja intensidad que copia los rasgos particulares que conforman el ojo. Por lo tanto, con el uso de cámaras de video de alta resolución, se trata de eliminar la aprehensión por parte de los usuarios: temor a los efectos colaterales que se puedan producir sobre el ojo.

Capítulo 2

TECNOLOGÍAS WEB

2.1. Internet, Web, Intranet y Extranet

La Internet, son millones de computadoras conectadas a redes de comunicación a nivel mundial, dichas redes se encuentran conectadas mediante ruteadores, los cuales permiten el envío de paquetes de información a su destino, vía cableado, fibra óptica ó microondas.

La Internet existe desde la década de los 60's y ha presentado un crecimiento exponencial desde finales de 1993, una vez que se pasó de una cobertura gubernamental y escolar a otra de todo tipo. Su crecimiento se estima en un rango del 200 al 300% al año.

Internet es descendiente de ARPAnet, red que creó la Agencia de Proyectos de Investigación Avanzados para la Defensa (DARPA) en los años sesenta, ARPAnet (y posteriormente Internet) estaba estructurada de tal modo que cada computadora estaba conectada a otras computadoras.

Los mensajes podían pasarse desde cualquier parte de la red a otra por distintas rutas, por lo que una sola interrupción en el sistema provocaba un número limitado de problemas.

Con el paso del tiempo, ARPAnet se convirtió en Internet, una red global que al principio utilizaban principalmente los científicos y las universidades. Al principio, la mayoría de los accesos se realizaban a través de texto y se conectaban en sistemas que utilizaban texto. El acceso a Internet con una orientación más gráfica que podían utilizar los consumidores era la conexión a un servidor en línea, como CompuServe, para obtener correo de Internet basado en texto.

En 1980, Timothy Berners-Lee, consultor del Laboratorio Europeo de Física de Partículas (CERN), creó un programa llamado "Enquire", que utilizaba "puntos interactivos" para realizar el seguimiento de las personas y de la información. En 1989, escribió un artículo en el que proponía que CERN creara un sistema basado en hipertexto para hacer seguimientos de la gran cantidad de información que recopilaba.

Éste fue el sistema que se convirtió en la World Wide Web o simplemente Web, la cual es una de las tantas subredes que posee Internet y se caracteriza por sus dos aplicaciones multimedia: Gopher y Http, que asemeja una telaraña, pues a medida que diversas instituciones públicas y privadas del mundo van adoptando esta tecnología, dicha red crece como si fuera una telaraña, pero de información (véase figura 2.1).

El Gopher es una aplicación que hace muy sencilla su utilización por el usuario, ya que, mediante un entorno gráfico permite la búsqueda y recuperación de archivos.

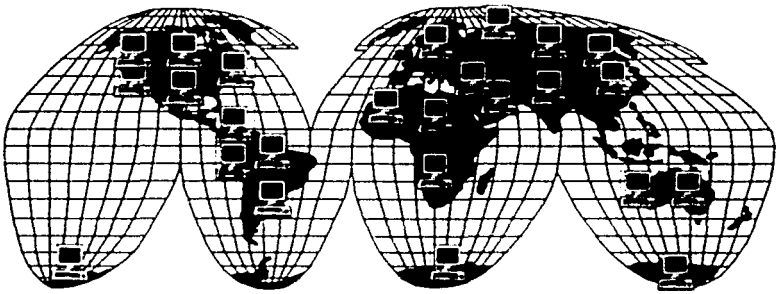


Figura 2.1
La telaraña Internet

La Web, además de presentar información en texto o imagen, permite la búsqueda de información a través de "hipertexto" o "ligas" y mediante el protocolo ftp, permite bajar o subir información en la red.

Modelo de 3 Capas

El modelo distribuido o modelo de tres capas está orientado al desarrollo de sistemas para Intranets, Extranets e Internet, y sus principales piezas son:

- *El servidor de base de datos.* Incorporar a todos los objetos encargados de mantener la integridad referencial así como el almacenamiento de la información de una manera segura para su recuperación y mantenimiento adecuados.
- *Uno o varios servidores de aplicaciones.* Contienen las Reglas del negocio, la lógica del funcionamiento del sistema, políticas y restricciones.
- *Los clientes.* Interactúan con el sistema mediante una interfase de usuario (UI) que generalmente es el navegador o visualizador de Internet.

En la figura 2.2 mostramos el esquema del modelo de tres capas.

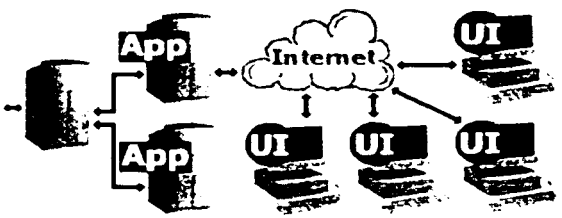


Figura 2.2
Esquema del modelo de tres capas

Intranet: Es un tipo de red que es menos conocida que la Internet, por la mayoría de la gente, y que está volviéndose cada vez más importante en el mundo. Una Intranet es una red de información a nivel corporativo o educativo. Es similar a la Internet, pero está enfocada a un grupo distinto de usuarios y presenta seguridad, de manera tal, que personas ajenas a la corporación no tienen acceso a su contenido.

Extranet: Es un tipo de red utilizada de manera tal, que una institución abre las puertas de su Intranet a sus clientes, proveedores, agentes de ventas. Una Extranet es básicamente un enlace privado y seguro entre dos o más negocios que usan la Internet como medio de comunicación y transferencia bidireccional de información.

Se utiliza para establecer comunicación entre dos o más negocios, entre sus empleados, así como comunicar aplicaciones de misión crítica comunes a ambas partes.

2.2 Internet Information Services (IIS)

Los Servicios para la Publicación de información en Internet (IIS), son una utilería incluida en el Sistema Operativo Windows NT 4.0, Workstation y 2000 Server, es propia de Microsoft y actualmente se encuentran en su versión 5.0, permite poner en marcha el servicio de Web, facilitando la publicación de Sitios Web, desde la Intranet hacia la Internet.

Permite, siempre y cuando se cuente con un Servidor de Web y una dirección IP homologada para ello, la creación de Sitios Web a través de directorios virtuales, a los cuales se podrá asignar asimismo permisos de sólo ejecución o de visualización de directorios y/o subdirectorios, según sea el caso.

Con IIS 5.0, es posible también administrar el Sitio Web de manera remota desde otra terminal que contenga Windows 2000 Server.

Algunas de las funcionalidades y herramientas más importantes que proporcionan IIS y Windows 2000 Server son:

- Páginas Activas en el Servidor (ASP), que no es más que el equivalente a la interfase CGI en el entorno de Microsoft. El aspecto que tienen los archivos ASP (con extensión .asp) cuando se encuentran en el servidor, es el de archivos de texto que contienen programas escritos en un lenguaje de sencilla sintaxis que integra HTML, SQL e instrucciones de VBScript. A dicho lenguaje, por extensión, se le denomina ASP. La integración de lenguajes en un mismo archivo hace mucho más homogéneo el proceso de desarrollo.
- Gestión de datos: El Servidor Activo define una arquitectura abierta para almacenar, gestionar y acceder a los datos en cualquier lugar de la red. Microsoft SQL Server es el sistema de gestión de bases de datos (SGBD) que se puede montar en el

servidor. OLE DB y ODBC proporcionan acceso a datos de otros SGBD como Oracle o DB2.

- Servicios de red: DCOM trabaja en colaboración con TCP/IP, http, CIFS y otros protocolos estándar para proporcionar interactividad en entornos de diversos fabricantes.

2.3 Lenguaje de Marcas de Hipertexto (HTML)

HTML: Son las siglas de HyperText Markup Language o Lenguaje de Marcas o etiquetas de Hipertexto y es bajo el cual operan en esencia las Páginas Web, el cual permite insertar dentro de un documento de texto órdenes especiales que, al ser interpretadas por un programa lector (o "navegador" de hoy en día), permiten variar los estilos de presentación de ese documento y relacionarlo con otros, que pueden estar en la misma computadora o en cualquier otra máquina conectada a Internet.

2.4 HTML Dinámico (DHTML)

HTML Dinámico (DHTML). No es una tecnología específica, como JavaScript, VBScript o ActiveX. Es más bien la reunión de diversas tecnologías, JavaScript, VBScript, Modelo de Objetos de Documento (DOM), Secciones (Layers), Hojas de Estilo en Cascada (CSS), con la finalidad de crear páginas que cambian aún cuando el medio en el cual se cargan sea el Visualizador ó Navegador.

Los principales elementos dentro del ámbito de DHTML tienen lugar del lado del Cliente.

2.5 Lenguaje de Etiquetas Expandible (XML)

Lenguaje de etiquetas expandible (XML), es un lenguaje surgido a partir de HTML, mientras que este se preocupa por el aspecto de los datos, XML se preocupa por su significado, ya que podemos crear etiquetas propias que describan con precisión lo que deseamos saber.

Los datos en XML no son solamente datos inteligentes, también son documentos inteligentes: *al visualizar la información, el nombre de modelo puede aparecer con una fuente diferente a la del nombre de un vendedor, o con el precio más bajo resaltado en verde*. A diferencia de HTML, el texto no tiene por qué ser presentado de manera uniforme. El texto inteligente XML puede controlar el contenido a transmitir.

XML tiene su origen en el Lenguaje Estandarizado de etiquetas (SGML). XML es de hecho un subconjunto directo de SGML, por tanto, la historia de SGML también es la de XML.

Los documentos XML están formados por elementos. Los elementos pueden constar de otros elementos así como de frases y palabras que normalmente se consideran como el texto del documento. XML denomina este texto los datos de carácter del documento y a toda la estructura, árbol de documento.

El elemento que contiene a los demás (por ejemplo: libro, informe o nota) recibe el apelativo de elemento raíz. Este nombre indica que es el único elemento que no depende de otro.

Los elementos incluidos en la raíz se llaman subelementos, que pueden contener a su vez subelementos. Si es así, se denominan ramas. De lo contrario, se llaman hojas.

Por tanto, los elementos capítulo y artículo son ramas (porque cuentan con subelementos), y en cambio los elementos párrafo y título son hojas (porque sólo contienen datos de carácter). Para referirse al elemento raíz también se utiliza la expresión elemento de documento porque engloba a todo el documento lógico. Los términos elemento raíz y elemento de documento se utilizan indistintamente.

A veces, los elementos incluyen información adicional llamada atributos, los cuales describen las propiedades de los elementos. Por ejemplo, un elemento de registro CIA incluye un atributo de seguridad que indica el nivel para ese elemento. Una base de datos de la CIA sólo dará acceso a determinados registros al personal autorizado que supere el nivel de seguridad establecido.

En la práctica, los documentos no siempre siguen a la perfección este modelo de árbol. Constan a menudo de características no jerarquizables como remisiones o enlaces de hipertexto de un artículo a otro del árbol. XML es capaz de representar estas estructuras. De hecho, XML va más allá de las potentes ligas proporcionadas por HTML.

La idea que subyace bajo el XML es la de crear un lenguaje muy general que sirva para muchos propósitos. El HTML está diseñado para presentar información directamente a los usuarios, y esto sin duda es algo bueno, pero es un lenguaje complicado de procesar para los programas informáticos. El HTML es limitado porque no indica lo que está representando, se preocupa principalmente de que eso tiene que ir en azul, o con un tipo de letra determinada, pero no te dice que lo que está mostrando es el título de un libro o el precio de un artículo. El XML hace precisamente esto: describe el contenido de lo que etiqueta.

La diferencia es clara en el siguiente ejemplo:

El llano en llamas
Juan Rulfo. Publicado en 1985.
Precio: $100.00. Ahorro del 12%

Ejemplo de los datos de un libro

El código en HTML es el siguiente:

```
<p align="center" style="margin-right:30.0pt;text-align:center"><b><span lang="EN-GB" style="font-
size:10.0pt;mso-bidi-font-size:9.0pt;color:#3366FF;
mso-ansi-language:EN-GB">El llano en llamas<o:p>
</o:p>
</span></b></p>
<p align="center" style="margin-right:30.0pt;text-align:center"><b><span lang="EN-GB" style="font-
size:10.0pt;mso-bidi-font-size:9.0pt;color:#3366FF;
mso-ansi-language:EN-GB">Juan Rulfo </span><span style="font-size:10.0pt;mso-bidi-font-
size:9.0pt;color:#3366FF">Publicado en 1985.<o:p>
</o:p>
</span></b></p>
<p align="center"><b><span style="font-size:10.0pt;mso-bidi-font-size:9.0pt;font-family:&quot;Times New
Roman&quot;,
mso-fareast-font-family:&quot;Times New Roman&quot;;color:#3366FF;mso-ansi-language:ES;
mso-fareast-language:ES;mso-bidi-language:AR-SA">Precio: $100.00. Ahorro del 12%</span></b>
```

y en XML lo podríamos escribir de la siguiente manera:

```
<?xml version="1.0"?>
<libro>
  <titulo>El llano en llamas</titulo>
  <autor>Juan Rulfo</autor>
  <publicacion>1985</publicacion>
  <precio cantidad="100.00" moneda="pesos"/>
  <descuento cantidad="12"/>
</libro>
```

Esto permitirá, por ejemplo, realizar motores de búsqueda mucho más eficaces, lo que nos permitirá un acceso más rápido y eficiente a la información. Nos permitirá acceder a nuestras páginas favoritas desde nuestro teléfono móvil, o desde la radio de nuestro coche, en el momento en el que los programas de reconocimiento de voz trabajen con XML. Facilitará el intercambio de información y la cooperación entre las empresas facilitando el comercio electrónico, etc. Y es que el XML busca precisamente crear la capacidad de hacerlo todo en la Web.

La potencia de esta forma de trabajar radica en que estamos etiquetando e identificando el contenido, olvidándonos en un principio por la forma de presentarlo. El Consorcio World Wide Web (W3C) desarrolló un lenguaje de hojas de estilo que nos lo permite, denominado Lenguaje de Estilo Expandible (XSL). Mediante una XSL podemos transformar un documento XML en otro XML, por ejemplo en HTML (véase figura 2.3).

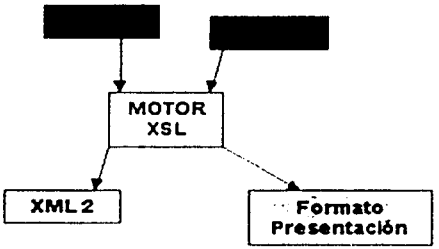


Figura 2.3
Transformación de un documento XML en HTML

2.5.1 HTML, XML versus SGML

Tampoco tenemos que equivocarnos y pensar que el XML es un HTML++. Tanto el XML como el HTML tienen su base en el SGML. El SGML (Standard Generalized Markup Language, ISO 8879) es el estándar internacional para la definición de la estructura y el contenido de diferentes tipos de documentos electrónicos. Es decir, es un metalenguaje que nos permite definir lenguajes para definir la estructura y el contenido de nuestros documentos. La definición de la estructura y el contenido de un tipo de documento se realiza en una DTD (definición de tipo de documento). En ella definimos los elementos que conformarán ese tipo de documentos y cómo tienen que estar organizados para que sea correcto. Por tanto, el HTML no es más que un tipo de documento SGML que se utiliza en la Web, y esto es importante, ya que aquí radica su principal diferencia con el XML.

El XML no es ningún tipo de documento SGML, sino que es una versión abreviada de SGML optimizada para su utilización en Internet (véase figura 2.4). Esto significa que con él vamos a poder definir nuestros propios tipos de documentos (podremos definir nuestras propias etiquetas) y, por tanto, ya no dependeremos de un único e inflexible tipo de documento HTML.

Figura 2.4
El XML como versión abreviada del SGML

El XML más que un HTML++ hay que considerarlo como un SGML-- optimizado para su utilización en Internet.

2.5.2 Lo que se necesita para usar XML

En realidad sólo hace falta un editor de textos, con el cual escribir nuestros documentos XML y DTD; y un procesador o parser XML. Existe un sin número de herramientas y aplicaciones para trabajar con XML las cuales pueden representar el fichero XML en forma de árbol, o en su formato original, por ejemplo:

- **XML Notepad.** Es un editor de XML desarrollado por Microsoft. Para su utilización es necesario tener instalado, como mínimo, la versión 4.01 del Explorer, aunque sólo podremos aprovecharlo en su totalidad con la versión 5.

- **Visual XML.** Es un editor de XML escrito en Java con JFC (Swing). Su autor es Pierre Morel.

- **XED.** Es un editor de XML desarrollado por Henry Thompson. Permite garantizar que el autor no va a escribir documentos que no estén bien formados y puede leer la DTD para sugerir la introducción de elementos válidos.

- **PSGML para Emacs.** Es un modo superior de Emacs para trabajar con SGML que se ha modificado para soportar XML. Lee la DTD, puede utilizar un analizador externo para validar documentos, realiza coloración de sintaxis y otras muchas cosas.

En estos, hay que diferenciar los que trabajan contra una DTD y, por lo tanto, validan el contenido de lo que escribimos y los que simplemente nos aseguran que el documento XML es bien formado, es decir, sintácticamente correcto respecto de las especificaciones del XML. La elección de uno u otro dependerá del tipo de documento que estemos escribiendo. Hay que aclarar que se está hablando de editores sencillos y al alcance de la mayoría de nosotros al ser gratuitos o muy baratos. Por supuesto existen editores muchos más complejos, que nos permiten editar nuestros documentos XML-SGML como si lo hiciésemos en un procesador de texto. Es el caso del ADEPT de ArborText o de las facilidades para trabajar sobre SGML/XML de la última versión de WordPerfect, y FrameMaker+SGML.

2.5.3 Parsers XML

Un parser o procesador de XML es la herramienta principal de cualquier aplicación XML. Mediante este parser no sólo podremos comprobar si nuestros documentos están bien

formados o válidos, sino que también podremos incorporarlos a nuestras aplicaciones, de manera que éstas puedan manipular y trabajar con documentos XML.

Actualmente hay muchos y para todos los lenguajes y plataformas: Java, C, Phyton, Visual Basic, Perl, Tcl, Delphi, etc. Todas las grandes compañías ya han elaborado sus propios procesadores de XML: IBM, Microsoft & Datachanel, Oracle, Sun. Y existen muchos más completamente gratis.

La utilización de uno u otro dependerá de nuestras necesidades, aunque es importante tener en cuenta la diferencia entre los que simplemente comprueban que el documento está bien formado, o el que valida respecto de una DTD.

2.5.4 Componentes de un documento XML

Elementos.

Todo documento XML se compone de uno o más elementos, cuyos límites están delimitados por etiquetas de comienzo y etiquetas de fin, en el caso de que tengan contenido:

```
<p>Mi Primer <destacar importancia ="1">documento XML</destacar></p>
```

y por una etiqueta de elemento vacío en el caso de ser elementos sin contenido:

```
<imagen fichero ="imagen.gif"/>
```

Cada elemento puede contener datos de carácter, elementos, ambas cosas a la vez o puede que estén vacíos (véase figura 2.5).

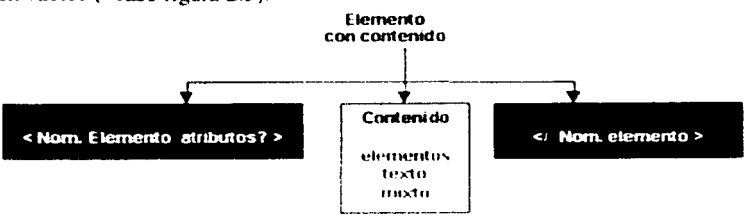


Figura 2.5
Elemento en un XML

En el caso de elementos con contenido, las etiquetas de comienzo se componen del símbolo menor que "<", el nombre del tipo de elemento, los atributos si los tiene y el símbolo mayor que ">". Mientras que las etiquetas de fin se componen del símbolo menor que seguido de contrabarra "</", el nombre del tipo del elemento y el símbolo mayor que " >".

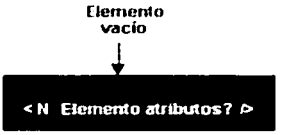


Figura 2.6
Elemento vacío

En el caso de ser un elemento vacío, solo hay una etiqueta de elemento vacío que se forma del símbolo menor que "<", el nombre del tipo de elemento, los atributos si los tiene y se cierra con el símbolo "/>" (véase figura 2.6). Es importante destacar este tipo de elementos, ya que hasta ahora en el SGML y, por tanto en el HTML entendido como aplicación SGML, los elementos vacíos sólo se representaban con una etiqueta de inicio.

Atributos.

Cada elemento puede tener atributos (propiedades) que nos ofrecen información sobre el elemento.

En nuestro ejemplo:

El elemento, "destacar" va caracterizado con el atributo "importancia", que nos indicará el grado de relevancia de su contenido.

El elemento "imagen" con el atributo "fichero", donde indicaremos el archivo que contiene la imagen.

```
<p>Mi Primer <destacar importancia="1">documento XML</destacar></p>
.....
<imagen fichero="imagen.gif" />
```

Como podemos observar, la definición de un atributo está formada por el nombre del atributo, seguido del símbolo igual "=" y, entrecomillado, el valor del atributo.

Prólogo.

Los documentos XML pueden empezar con un prólogo, en el que esencialmente se define:

- Una declaración XML
- Una declaración de tipo de documento

Ejemplo:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE documento [
```

```
<!ELEMENT documento (p | imagen | ejemplo)*>
<!ELEMENT p (#PCDATA|destacar)* >
<!ELEMENT destacar (#PCDATA)>
<!ATTLIST destacar importancia CDATA #REQUIRED>
<!ELEMENT imagen EMPTY>
<!ATTLIST imagen
            fichero CDATA #REQUIRED>
<!ELEMENT ejemplo (#PCDATA)>
]>
```

En la declaración XML:

```
<?xml version="1.0" encoding="UTF-8"?>
```

Indicamos información sobre la versión de XML que estamos utilizando. Por el momento sólo puede ser la versión 1.0. Y también indicamos información sobre el tipo de codificación de caracteres que estamos utilizando. En nuestro caso es el código ASCII de 7 bits, que es un subconjunto del código Unicode denominado UTF-8. No hubiese sido necesario declararlo, ya que es el que los parsers manejan por defecto.

En la declaración del tipo de documento:

```
<!DOCTYPE documento [
<!ELEMENT documento (p | imagen | ejemplo)*>
<!ELEMENT p (#PCDATA|destacar)* >
<!ELEMENT destacar (#PCDATA)>
<!ATTLIST destacar importancia CDATA #REQUIRED>
<!ELEMENT imagen EMPTY>
<!ATTLIST imagen  fichero CDATA #REQUIRED>
<!ELEMENT ejemplo (#PCDATA)>
]>
```

asociamos la DTD respecto de la cual construimos el documento. Puede ir implícita en el propio documento XML, aunque también puede hacerse externa al documento e incluso de una forma mixta. Si la hubiésemos escrito en un fichero "ejemplo.dtd" se tendría que referenciar de la siguiente manera:

```
<!DOCTYPE documento SYSTEM "ejemplo.dtd">
```

Ambas partes del prólogo son opcionales, aunque en el caso de incluir ambas la declaración XML tiene que ir antes.

Comentarios.

Mediante los cuales podemos proporcionar información que el parser no tendrá en cuenta.

```
<!-- Esto es un comentario -->
```

Los comentarios empiezan con los caracteres "<!--" y terminan con "-->" y pueden colocarse en cualquier sitio excepto dentro de las declaraciones, etiquetas y otros comentarios.

CDATA.

Permiten integrar texto en un documento en XML que de otra forma sería interpretado como etiquetas. Es decir, estamos introduciendo texto que luego el procesador XML va a mostrar pero no va a procesar como marcado.

```
<![CDATA[
        Aquí puedo poner lo que quiera.
]]>
```

Los CDATA empiezan con los caracteres "<![CDATA[" y termina con "]]>".

Dentro de ellos podemos colocar cualquier cosa ya que no va a ser interpretado, con la salvedad de la cadena que indica el final de CDATA, "]]>", ya que el procesador al encontrársela entendería que la sección CDATA ya ha terminado con las nefastas consecuencias que esto puede tener.

Entidades predefinidas.

En XML existen algunos caracteres reservados que no podemos utilizar para evitar problemas con el marcado, lo que no significa que no tengan que salir en nuestros documentos XML.

En nuestro ejemplo, nos aparece el caso cuando intentamos escribir la etiqueta <documento>

```
<p>Comienza con la etiqueta &lt;documento&gt;</p>
```

Ya hemos visto que una posible solución es la utilización de CDATA, pero sin duda es poco útil cuando simplemente queremos escribir un carácter.

Las entidades predefinidas son marcas XML que se utilizan para representar estos caracteres. El XML especifica cinco entidades predefinidas:

- & para el &
- < para el <
- > para el >
- ' para el '
- " para el "

Como podemos observar, se reconocen al ir entre los símbolos "&" y ";".

2.5.5 Documentos bien formados y documentos válidos

Como se dijo anteriormente, a diferencia del SGML, no es necesario que un documento XML esté asociado a una DTD. Por tanto, en función de si lleva asociada una DTD o no, podemos diferenciar dos tipos de documentos XML:

- Válidos, aquellos que siguen las reglas de una DTD especifica.
- Bien formados (well-formed), que no tienen necesariamente una DTD asociada, pero siguen las reglas del XML al pie de la letra.

Evidentemente, los documentos válidos son bien formados.

Documentos XML bien formados

Como se habia dicho anteriormente, en una DTD definimos cómo va a ser un tipo de documento; es decir, definimos los elementos, atributos y entidades que lo van a formar, cómo se estructuran y relacionan. Por tanto, si en la elaboración de nuestros documentos XML no utilizamos ninguna, el parser no puede proporcionarnos información sobre la validez de ese documento; es decir, no nos puede indicar que los elementos y atributos que utilizamos son los correctos y que se encuentran en el orden adecuado, si no que, simplemente nos indicará si ese documento está bien formado o no: es decir, si respeta las reglas sintácticas del lenguaje XML.

Según la especificación, un objeto de texto es un documento XML bien formado si:

- Tomado como un todo, cumple la regla denominada "document".
- Respeta todas las restricciones de buena formación dadas en la especificación.
- Cada una de las entidades analizadas que se referencia directa o indirectamente en el documento está bien formada.

La regla "document"

Cumplir la regla "document" antes mencionada significa:

- Que contiene uno o más elementos.
- Hay exactamente un elemento, llamado raíz, o elemento documento, del cual ninguna parte aparece en el contenido de ningún otro elemento.
- Para el resto de elementos, si la etiqueta de comienzo está en el contenido de algún otro elemento, la etiqueta de fin está en el contenido del mismo elemento. Es decir, los elementos delimitados por etiquetas de principio y final se anidan adecuadamente mutuamente.

El siguiente ejemplo no es un documento XML bien formado:

```
Mi primer documento XML.
```

ya que no contiene ningún elemento y, por lo tanto, está incumpliendo la regla número 1.

En cambio:

```
<p>Mi primer documento XML.</p>
```

sí que lo es, al contener al menos el elemento "p". La principal razón por la que el procesador comprueba los elementos es para determinar si el documento tiene estructura de datos que pueda extraer. Un documento que carece de elementos no tiene estructura de datos. Un documento con al menos un elemento tiene estructura de datos. En cambio:

```
<p>Mi primer documento XML.</p>
<p>Mi primer documento XML.</p>
```

no es un documento XML bien formado al incumplir la regla número 2, según la cual sólo puede existir un único elemento raíz.

Aunque escrito de la siguiente manera sí que es correcto:

```
<documento>
        <p>Mi primer documento XML.</p>
        <p>Mi primer documento XML.</p>
</documento>
```

al convertirse el elemento "documento" en el elemento raíz, ser único y no formar parte del contenido de ningún otro elemento. En cambio, el siguiente ejemplo:

```
<documento>
        <p>Mi primer <destacar>documento XML.</p></destacar>
        <p>Mi primer documento XML.</p>
</documento>
```

es incorrecto al incumplir la regla 3, ya que la etiqueta inicio del elemento "destacar" está dentro del contenido del elemento "p", pero su etiqueta final está fuera. La forma correcta sería la siguiente:

```
<documento>
        <p>Mi primer <destacar>documento XML.</destacar></p>
        <p>Mi primer documento XML.</p>
</documento>
```

Además, se observan algunas diferencias entre el XML con el HTML:

Utilizo etiquetas propias. Y es que en XML no se esta trabajando con etiquetas predefinidas. Se puede crear un propio lenguaje de etiquetas en función de las necesidades.

La sintaxis es estricta. No se permite dejar de entrecomillar los atributos o utilizar las mayúsculas y minúsculas sin ningún control. La especificación XML determina claramente una serie de reglas que especifican cuando un documento está bien formado.

La utilización de una DTD. En HTML, a pesar de ser una aplicación SGML, no era obligatorio utilizarlas y aunque para trabajar con XML tampoco será necesario, sí que será recomendable. Posiblemente no acompañen al documento XML en su distribución, pero resultan muy útiles en la elaboración y validación de los documentos.

Los elementos vacios. Son los elementos del tipo <img>, <hr>, etc. de HTML, en los que no existe etiqueta final al no tener contenido. Ahora, en el XML, la propia etiqueta de inicio llevará una contrabarra al final que los identificará.

2.5.6 Modelo de Objeto de Datos (DOM)

DOM define un conjunto estándar de comandos que los analizadores exponen para facilitarle el acceso al contenido de los documentos HTML y XML desde sus programas. Un analizador de XML compatible con DOM toma los datos de un documento XML y los expone mediante un conjunto de objetos que se pueden programar, según lo expuesto por el Analizador XML de Microsoft (Msxml.dll). DOM para XML es un modelo de objeto que muestra el contenido de un documento XML. La especificación de nivel 1 del Modelo de objeto de documento (DOM) del W3C define actualmente lo que debería mostrar un DOM como propiedades, métodos y eventos. La implementación de Microsoft del modelo DOM es totalmente compatible con el estándar del W3C y tiene características adicionales que facilitan el trabajo con archivos XML desde los programas.

Para utilizar XML DOM, hay que crear una instancia de un analizador XML. Para ello, Microsoft muestra XML DOM mediante un conjunto de interfaces COM estándar en Msxml.dll. El archivo Msxml.dll contiene la biblioteca de tipos y el código de implementación para trabajar con documentos XML.

2.5.7 Codificación de datos XML

Muchos usuarios desconocen la forma de hacer que los archivos XML transfieran datos correctamente entre plataformas distintas. Estos usuarios crean un documento XML, introducen datos, incluyen unas etiquetas, les da la forma adecuada e incluso insertan la declaración <?xml version="1.0"?> para una medición correcta. A continuación, intentan cargarlo pero, una vez realizado, reciben un mensaje de error inesperado del Analizador XML de Microsoft (MSXML), en el que se indica que existe un problema con los datos. Esto puede resultar frustrante para el autor del nuevo XML, ya que cree que esta operación debería funcionar.

Sin embargo, esto no es totalmente cierto. Es probable que el mensaje de error inesperado de MSXML sea debido a que la plataforma que recibe los datos los almacena de forma distinta a la plataforma desde la que se han enviado, lo que causa problemas en la codificación de caracteres.

2.5.8 Formatos de datos para varias plataformas

La creación de tecnologías de plataformas múltiples y el permitir que distintas plataformas compartan los datos constituyen un conflicto con el que las industrias de software y hardware se han enfrentado desde el momento en que consiguieron establecer la conexión entre dos equipos. Desde un principio, todo se ha vuelto cada vez más complicado debido al aumento del número de tipos de equipos, las distintas formas de conectarlos y los distintos tipos de datos que se desean compartir entre ellos.

Tras décadas de investigación en las tecnologías de programación de plataformas múltiples, la única solución de plataformas múltiples real (y probablemente la única todavía durante mucho tiempo) es la que se obtiene mediante *formatos de datos estándar* simples. El éxito del Web se ha basado en estos formatos exactamente. Hoy en día, el principal objeto que pasa entre los servidores y los exploradores de Web es el encabezado HTTP y las páginas HTML, los cuales son formatos de texto estándar.

2.5.9 Codificación de caracteres

Los formatos de texto estándar se generan en juegos de caracteres estándar. Hay que recordar que todos los equipos almacenan el texto como números. Sin embargo, distintos sistemas pueden almacenar el mismo texto con distintos números. En la siguiente tabla, se muestra cómo se almacena un intervalo de bytes, primero en un equipo normal que utiliza Microsoft Windows® utilizando la página de código predeterminada 1252 y después en un equipo normal de Apple® Macintosh® con la página de código Latina de Macintosh (véase figura 2.7).

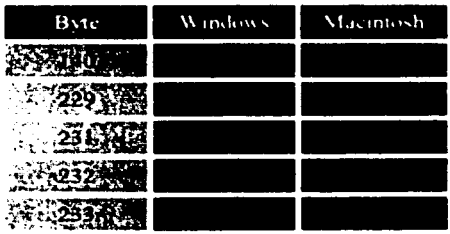


Figura 2.7
Un caracter en distintas páginas de código

Por ejemplo, si un usuario de Macintosh, residente en Suecia realiza un pedido en http://www.barnesandnoble.com/, puede que desconozca que su equipo almacena los caracteres de forma distinta que el nuevo servidor Web de Windows 2000. Por lo tanto, cuando escriba su domicilio de Suecia en el campo de dirección de envío del formulario de pedido, creerá que Internet enviará el carácter å correctamente (valor de byte 140 en Macintosh), sin saber que el mensaje se recibirá y procesará a través de equipos que traducen el valor de byte 140 como la letra (E).

2.5.10 Unicode

El grupo Unicode Consortium (en inglés) decidió que sería buena idea definir una página de códigos universal (que utiliza 2 bytes en lugar de uno por carácter) que cubra todos los idiomas del mundo, para solucionar el problema de asignación entre distintas páginas de códigos.

Entonces, si Unicode soluciona los problemas de codificación de caracteres entre múltiples plataformas, ¿por qué no se ha convertido en el único estándar? El primer problema radica en que al cambiar a Unicode, algunas veces implica el doblar el tamaño de todos los archivos, lo que en un mundo de enlaces por red no es precisamente ideal. Por lo tanto, algunos usuarios prefieren utilizar los juegos de caracteres de un solo byte más antiguos, como desde ISO-8859-1 hasta ISO-8859-15, Shift-JIS, EUC-KR, etc.

El segundo problema consiste en que aún existen demasiados sistemas que no se basan en Unicode, lo que significa que en una red, algunos de los valores de byte que forman los caracteres Unicode pueden causar problemas importantes en estos sistemas antiguos. Por lo tanto, se han definido los formatos de transformación Unicode (UTF); utilizan técnicas de desplazamiento de bits para codificar caracteres Unicode como valores de byte que serán "transparentes" (o que circularán con seguridad) en esos sistemas más antiguos.

La codificación de caracteres más utilizada es UTF-8. UTF-8 toma los primeros 127 caracteres del estándar Unicode (que son los caracteres latinos básicos, A-Z, a-z y 0-9, y algunos caracteres de puntuación) y los asigna directamente a valores de un solo byte. A continuación, aplica una técnica de desplazamiento de bits, utilizando el bit alto de los bytes para codificar el resto de los caracteres Unicode. El resultado de todo esto es que el carácter sueco å (0xE5) se convierte en el galimatías de 2 bytes Ã¥ (0xC3 0xA5). Así que, a menos que se puedan realizar desplazamientos de bits en la cabeza, el ser humano no puede leer la codificación de datos en UTF-8

2.5.11 Encabezado de tipo y contenido

Puesto que los anteriores juegos de caracteres de un byte todavía se utilizan, el problema de la transferencia de datos no se solucionará hasta que hayamos especificado en qué juego se encuentran los datos. Al reconocer esto, los grupos de protocolos HTTP y de correo electrónico de Internet han definido una forma estándar para especificar el juego de

caracteres en la propiedad Contenido-Tipo del encabezado del mensaje. Esta propiedad especifica un juego de caracteres de la lista de los nombres de juegos de caracteres registrados, definidos por la Autoridad para la Asignación de Nombres en Internet (IANA). Un encabezado HTTP común puede contener el siguiente texto:

```
HTTP/1.1 200 OK
Content-Length: 15327
Content-Type: text/html; charset=ISO-8859-1,
Server: Microsoft-IIS/5.0
Content-Location: http://www.microsoft.com/Default.htm
Date: Wed, 08 Dec 1999 00:55:26 GMT
Last-Modified: Mon, 06 Dec 1999 22:56:30 GMT
```

Este encabezado le indica a la aplicación que lo siguiente se encuentra en el juego de caracteres ISO-8859-1.

2.5.12 Metaetiquetas de contenido y tipo

La propiedad Contenido-Tipo es opcional y en algunas aplicaciones, se elimina la información del encabezado HTTP y sólo aparece HTML. Para solucionar esto, el grupo de estándares HTML definió una metaetiqueta opcional como un modo de especificar el juego de caracteres en el propio documento HTML, para que éste fuese autodescriptivo.

```
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=ISO-8859-1">
```

En este caso, el juego de caracteres ISO-8859-1 declara que en esta página HTML concreta, el valor de byte de 229 significa å. Esta página carece de ambigüedad en cualquier sistema y los datos no se malinterpretan. Por desgracia, debido a que esta metaetiqueta es opcional, aún se producen errores.

2.5.13 Entidades de caracteres

No todos los sistemas admiten todos los juegos de caracteres registrados. Por ejemplo, no es probable que muchas plataformas admitan el juego de caracteres de gran sistema (mainframe) IBM, denominado EBCDIC. Windows NT lo hace, aunque no parece que sea un caso frecuente, lo que es la razón más lógica por la que la página principal *http://www.ibm.com* se genera en ASCII.

Como plan de seguridad, HTML permite la codificación de caracteres individuales en la página a través de la especificación del valor del carácter Unicode exacto. A continuación, estas entidades de caracteres se analizan, independientemente del juego de caracteres, y los

valores Unicode se pueden determinar sin ambigüedad. La sintaxis para esto es "&=229;" o "å".

2.5.14 Juegos de caracteres y MSXML DOM

Una vez tratadas las distintas formas de codificar los caracteres, hay que observar la forma de cargar documentos XML en MSXML DOM y los tipos de mensajes de error que se pueden recibir cuando se encuentran caracteres con codificación ambigua. Los dos métodos principales para cargar documentos XML DOM son el método LoadXML y Load.

El método LoadXML siempre toma BSTR Unicode codificado en UCS-2 ó sólo UTF-16. Si intenta pasar algo que no sea un BSTR Unicode válido a LoadXML, no se podrá cargar.

El método Load implementa el siguiente algoritmo para determinar la codificación de caracteres o el juego de caracteres del documento XML:

- Si el encabezado de contenido y tipo HTTP define un juego de caracteres, éste anula todo lo existente en el documento XML.
- Si existe una marca de orden de byte Unicode de 2 bytes, se considera que la codificación es UTF-16.
- Si existe una marca de orden de byte Unicode de 4 bytes, se considera que la codificación es UTF-32.
- De lo contrario, se considera que la codificación es UTF-8, a menos que detecte una declaración XML con un atributo de codificación que especifica otro juego de caracteres (como ISO-8859-1, Windows-1252, Shift-JIS, etc.).

Existen dos errores que se devolverán desde XML DOM y que indican problemas de codificación. El primero suele indicar que un carácter en el documento no coincide con la codificación del documento XML:

- Se encontró un carácter no válido en el contenido del texto.

El objeto ParseError indicará el lugar exacto en una línea concreta en donde se produce este carácter incorrecto, para que pueda solucionar el problema.

El segundo error indica que ha comenzado con una marca de orden de byte Unicode (o ha utilizado el método LoadXML) y, a continuación, un atributo de codificación no ha especificado una codificación de 2 bytes (como UTF-8 ó Windows-1250):

- No se admite cambiar de una codificación actual a una codificación especificada.

Asimismo, puede haber utilizado el método Load e iniciado con una codificación de un único byte (sin marca de orden de byte), pero posteriormente se encontró un atributo de codificación que especificaba una codificación de 2 ó 4 bytes (como UTF-16 ó UCS-4).
En pocas palabras, no puede cambiar entre un juego de caracteres de bytes múltiples, como UTF-8, Shift-JIS o Windows-1250, y codificaciones de caracteres Unicode como UTF-16, UCS-2 ó UCS-4 utilizando el atributo de codificación en una declaración XML, puesto que la propia declaración debe utilizar el mismo número de bytes por carácter que el resto del documento.

2.5.15 Creación de documentos XML con MSXML

Una vez cargado el documento XML, se puede manipular utilizando DOM sin preocuparse de los aspectos de codificación, ya que el documento se almacena en la memoria como Unicode. Todas las interfaces XML DOM se basan en BSTR COM, que son cadenas Unicode de 2 bytes. Esto significa que puede generar un documento MSXML DOM en la memoria que contenga cualquier tipo de caracteres Unicode y todos los componentes podrán compartir este DOM en la memoria, sin ninguna confusión acerca del significado de los valores de los caracteres Unicode. Sin embargo, cuando lo guarde, MSXML codificará todos los datos en UTF-8 de forma predeterminada. Por ejemplo, imagine que realiza lo siguiente:

```
var xmldoc = new ActiveXObject("Microsoft.XMLDOM")
var e = xmldoc.createElement("test");
e.text = "Â",
xmldoc.appendChild(e),
xmldoc.save("foo.xml"),
```

Se producirá el siguiente archivo con codificación UTF-8:

```
<test>ÂÝ</test>
```

Nota: El ejemplo anterior sólo funcionará si ejecuta el código fuera del entorno del explorador. Si utiliza el método Save mientras se encuentra dentro del explorador, no se producirán los mismos resultados debido a restricciones de seguridad.

Aunque pareciera extraño, esto es correcto. La siguiente prueba carga el archivo con codificación UTF-8 y comprueba si UTF-8 se descodifica al valor de carácter Unicode 229:

```
var xmldoc = new ActiveXObject("Microsoft.XMLDOM")
xmldoc.load("foo.xml"),
if (xmldoc.documentElement.text.charCodeAt(0) == 229)
{
   WScript.echo("Yippee - it worked !!"),
}
```

Para cambiar la codificación que el método Save de XML DOM utiliza, necesita crear una declaración XML con el siguiente atributo de codificación en la parte superior del documento:

```
var pi = xmldoc.createProcessingInstruction("xml",
                " version='1.0' encoding='ISO-8859-1'");
xmldoc.appendChild(pi);
```

Cuando se utilice el método save, se recibirá el siguiente archivo con codificación ISO-8859-1:

```
<?xml version= "1.0" encoding="ISO-8859-1"?>
<test>á</test>
```

Sin embargo, hay tener cuidado de no permitir que la propiedad XML le confunda. Ésta devuelve una cadena Unicode. Si utiliza la propiedad XML en el objeto DOMDocument tras crear la declaración de codificación ISO-8859-1, recibirá la siguiente cadena Unicode:

```
<?xml version="1.0"?>
<test>á</test>
```

Hay que observar que la declaración de codificación ISO-8859-1 ha desaparecido. Se trata de algo normal. La razón de ello es que puede volver y llamar LoadXML con esta cadena y funcionará. De lo contrario, LoadXML generará un error con el mensaje: "No se admite cambiar de una codificación actual a una codificación especificada."

2.6 Patrones Lenguaje Extensible de Hojas de Estilo (XSL)

Se ha mencionado que el XML se encarga de estructurar la información; sin embargo, XML estaría "incompleto" si se dejara de lado otro asunto importante: los usuarios nos sentimos más cómodos cuando el formato no es tan explícito y nos gusta ver documentos diagramados con criterios estéticos más que informáticos. Desde el punto de vista de quien crea una publicación, sería interesante contar con algún tipo de mecanismo estándar para dar el formato a partir de la estructura. Esto es XSL (eXtensible Stylesheet Language - Lenguaje extensible de hojas de estilo), un lenguaje para procesar estructuras y convertirlas en textos con legibilidad adecuada.

XML es un estándar para denotar explícitamente la estructura de un texto. XSL es un estándar para convertir esa estructura a un formato adecuado para la lectura.

2.6.1 Transformaciones del Lenguaje XSL (XSLT)

El XSLT es un lenguaje que nos permite convertir documentos XML en documentos XML o HTML (véase figura 2.8). La forma de llevar a cabo esto es mediante hojas de estilo (stylesheets), los cuales son documentos XML especializados que utilizan elementos y atributos que describen los cambios que se desean llevar a cabo. La definición de estos elementos y atributos especializados provienen del W3C, los mismos responsables de los estándares del XML y HTML.

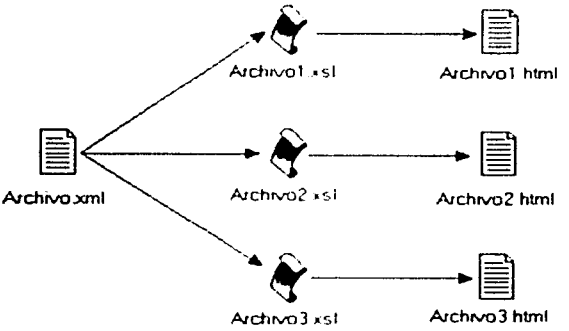


Figura 2.8
Conversión de un XML en un HTML, a través de un XSL.

El XSLT es parte del XSL. La especificación XSL se describe como un lenguaje con dos partes: un lenguaje para transformar documentos XML y un vocabulario XML para describir como dar formato al contenido del documento. Pero debido a que este lenguaje tenía un poder de formato que iba más allá como el incorporar elementos especiales para borrar, renombrar o reordenar documentos, fue que el grupo de trabajo de XSL del W3C decidió separar este tipo de transformaciones en el lenguaje XSLT con sus especificaciones por separado.

XSLT es un estándar, y esto es una ventaja dado que múltiples vendedores trabajan sobre él al mismo tiempo, contribuyendo a su diseño. Todas las bondades del XSLT y su soporte en diferentes plataformas reflejan el alto grado de interés; mientras que la disponibilidad de implementaciones de códigos abiertos hacen fácil al programador la tarea de disponer de su propio procesador XSLT personificado.

2.6.2 Documentos, árboles y transformaciones

Un XSLT describe la forma de cómo se transforma un árbol fuente en un árbol resultado. Y la verdad es que el XSLT ofrece gran flexibilidad dado que el árbol fuente no necesariamente debe ser un archivo en disco duro. La entrada puede provenir de un árbol DOM en memoria o de cualquier fuente capaz de crear un árbol fuente. Similarmente, el procesador no tiene que escribir el resultado en un archivo en disco, sino que lo puede generar como un árbol DOM, para después poder ser procesado o no por otra hoja de estilos XSLT (véase figura 2.9).

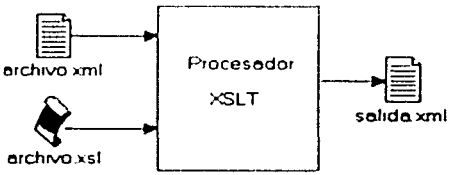


Figura 2.9
Procesador XSLT

Una transformación XSLT se especifica por un XML bien formado llamado hoja de estilo. Los elementos clave de esta hoja de estilos son ciertos elementos especializados contenidos en el namespace del XSLT. Un namespace es un nombre único para un conjunto dado de nombres de elementos y atributos. Se declaran normalmente en el XML con un alias que usa este documento como prefijo para los nombres del namespace.

Los XSLT usualmente utilizan "xsl" como prefijo para el namespace, de esta forma, los elementos xsl: text ó xsl: message se dirá que provienen del namespace XSLT.

Una hoja de estilo XSLT tiene una colección de plantillas de regla (template rules); cada plantilla de regla tiene cierto patrón que identifica los nodos del árbol fuente para los cuales se aplicará la plantilla, y la plantilla en sí la cual procesará a los nodos resultantes. En otras palabras, un elemento xsl :template le dice al procesador XSLT: "al avanzar a través del árbol, si encuentras un nodo cuyo nombre coincida con el que estoy indicando en el atributo "match", agrega mi contenido al árbol resultante" (véase figura 2.10).

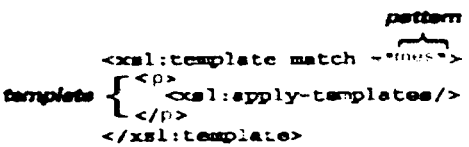


Figura 2.10
Ejemplo de una plantilla

2. 6.3 Origen del XHTML

Cualquier observador de la Web puede comprobar fácilmente que la mayoría de las páginas web existentes en Internet presentan código mezcla del estándar HTML y de las especificaciones particulares de los editores-navegadores utilizados en cada caso, siendo en algunos casos verdaderos ejemplos de mala programación y poca atención, aunque sean visualmente aptos.

No es muy difícil deducir que la existencia y utilización de etiquetas no especificadas por las normas (en la actualidad, la última versión de la normativa que regula el código HTML es la 4) y el consentimiento de "faltas de gramática HTML" por los navegadores, lleva a un punto difícil de controlar, por lo que, aprovechando la inercia que ha generado (y que generará) la publicación del estándar XML (Extensible Markup Language), mucho más estricto con las reglas del código, los perseverantes e indesmallables gestores del W3C están trabajando en unas reglas que terminen con parte de este desajuste actual.

Esta nueva normativa se denomina XHTML (Extensible HyperText Markup Language), y describe las especificaciones que deben tenerse en cuenta para generar un código estricto que no se salga de las reglas gramaticales que debe contener una página web HTML bien realizada.

Por supuesto que esta normativa no resuelve todos los problemas del HTML, como la existencia de etiquetas "propietarias" o el diferente soporte de CSS o JavaScript, pero sí ayudará a eliminar los errores gramaticales, unificando la descripción del código y facilitando la portabilidad de los documentos. Todo navegador que se precie y todo editor HTML que desee mantener un lugar de prestigio, deberá ajustarse a sus normas, que por otro lado son muy sencillas de seguir, como veremos más adelante.

En realidad, el usuario no notará nada en especial si decide generar código XHTML en vez de HTML, ya que las etiquetas no cambian. Si realiza su diseño "a mano", o sea, con un editor ASCII, solo tendrá que tener cuidado en seguir las reglas de la especificación. Si utiliza un editor WYSIWYG para crear sus páginas web, será el propio editor el encargado de generar el código adecuado, tal como ocurre en los editores actuales.

En cuanto a los navegadores, cuando lean la línea de código que especifica la adecuación a las normas del XHTML, aplicarán el DTD (Document Type Definition) correspondiente, menos permisivo que el que aplican en la actualidad, pero de riguroso estándar.

2.6.4 Relación con HTML y XML

Se puede decir sin lugar a dudas que el XHTML está perfectamente interrelacionado con el XML y HTML, cogiendo lo mejor de cada uno, o sea, las conocidas y extendidas etiquetas del HTML y la estricta normativa del XML.

Matemáticamente, se podría decir que: XML + HTML = XHTML (más o menos) <-- expresión poco técnica, pero efectiva.

Por si existe alguna duda en cuanto a la paternidad y origen de los estándares XML, HTML y XHTML, se pueden resumir en:

- XML es una simplificación del SGML (Standard Generalized Markup Language), eliminando todo lo que no es necesario para su utilización en Internet, pero manteniendo sus características más potentes e importantes. Es un metalenguaje, esto es, un lenguaje capaz de generar otros lenguajes.
- HTML es un lenguaje de marcas, subconjunto del SGML, diseñado para publicar documentos en la Web con la máxima sencillez.
- XHTML es una reformulación de HTML 4 para adaptarse a las normas del XML.

Aunque los orígenes son los comentados, ya se ha expuesto que la situación actual, en lo que respecta al HTML, no coincide con la idea original. Por este motivo, el W3C ha sido el responsable de tomar la decisión de reformular el HTML 4 para adaptarse al XML (solución muy fácil), en vez de crear un nuevo HTML que volviese al redil del SGML (solución mucho más difícil de imponer) o aconsejar que se utilice el ya existente SGML (realmente mucho más complejo y difícil de utilizar).

Las razones esgrimidas por el W3C para aconsejar el uso del XHTML son dos, principalmente:

- XHTML, ya que es una aplicación XML, ha sido diseñado para ser ampliable (de ahí el añadido de la palabra Extensible). Esto significa que se pueden añadir nuevas etiquetas o elementos sin alterar la DTD en la que está basado el análisis del documento.
- XHTML ha sido diseñado pensando en la portabilidad. Aunque hoy en día la unión de la potencia de los ordenadores y de los navegadores es suficientemente para asumir las posibles diferencias y pequeños errores del código HTML, se espera que para los próximos años se produzca un aumento considerable de los aparatos que sean capaces de tratar información en código HTML, no disponiendo estos de dicha potencia. Televisiones, teléfonos móviles, ordenadores de bolsillo, calculadoras, hornos, tostadoras, etc., soportarán código HTML, siempre que este realmente unificado y se ajuste a normas estrictas para no dar problemas que exijan soluciones complejas.

2.6.5 Diferencias con HTML

Las normas que regulan el código XHTML son suficientemente sencillas como para no asustar a nadie, sobre todo si se es un profesional del diseño web y/o de la programación.

Las diferencias principales entre el clásico HTML y el nuevo XHTML son:

- Toda la descripción del código debe estar en minúsculas.

Mientras el XML es sensible a utilización de las mayúsculas y de las minúsculas (las etiquetas <COCHE>, <Coche> y <coche> son diferentes) y el HTML es indiferente a la utilización de ambos tipos de letras (las etiquetas del ejemplo del coche serían iguales), las etiquetas del código XHTML deben estar siempre en minúsculas.

Esto no es problema alguno para los diseñadores que trabajan directamente con editores sencillos, y si crean sus documentos con editores automatizados, la mayoría de ellos soportan opciones capaces de pasar elementos definidos en mayúsculas a minúsculas de forma automática, realizando la conversión de un documento antiguo al nuevo estándar sin intervención del usuario.

En la figura 2.11 se puede ver un ejemplo práctico sobre este punto.

HTML	XHTML
<BODY BgColor="#FFFFFF">	<body bgcolor="#ffffff">

Figura 2.11
Toda la descripción del código debe estar en minúsculas

En este punto existe una excepción, ya que los valores de los atributos definidos por el usuario pueden estar igualmente en mayúsculas como en minúsculas. En el ejemplo anterior, el código XHTML podría ser <body bgcolor="#FFFFFF"> sin mayor problema.

- Todos los valores de los atributos deben ir entrecomillados.

Ya no se permiten ambigüedades ni olvidos con respecto a la descripción de los valores de los atributos. Aunque sean numéricos, deben ir entre comillas, dobles (") o sencillas (').

En la figura 2.12 se puede ver un ejemplo práctico sobre este punto.

HTML	XHTML
<TABLE BORDER=2>...	<table border="2">...

Figura 2.12
Todos los valores de los atributos deben ir entrecomillados

- Todos los elementos "no vacíos" deben ir entre la etiqueta de principio y la etiqueta de final.

Todos los diseñadores acostumbrados a poner una única etiqueta <P> para terminar un párrafo deben olvidarse de esa costumbre, ya que en XHTML es obligatorio utilizar la etiqueta de principio <P> y la de final </P>. Esto es aplicable a todos los casos, incluidos los <LI>, <DT> y <DD>, que ahora deben definirse como <li> ... , <dt> ... </dt> y <dd> ... </dd>.

En la figura 2.13 se puede ver un ejemplo práctico sobre este punto.

HTML	XHTML
Texto 1<P>	Texto 1
Texto 2<P>	Texto 2
...	...

Figura 2.13
Todos los elementos "no vacíos" deben ir entre la etiqueta de principio y la etiqueta de final

- Los elementos "vacíos" deben llevar terminación.

Un elemento vacío, como su propio nombre indica es el que no tiene contenido.

Lo normal es que los elementos si tengan contenido entre las etiquetas de principio y de final, y así, las etiquetas y contienen un párrafo, las etiquetas y contienen un texto en cursiva, etc.

No obstante, en HTML también existen algunos elementos que no contienen nada, como
, <hr> e <img>, por lo que solo existen como etiquetas únicas, que hacen las veces de principio y de final.

Pues bien, en XHTML no se permite la existencia de elementos sin terminación, por lo que los elementos vacíos incluyen su propia terminación en la misma etiqueta. El problema se resuelve añadiendo un "espacio" y una "barra" ( ) justo antes del signo "mayor" ( )

Según lo dicho, los ejemplos anteriores quedan en XHTML como se muestra en la figura 2.14.

HTML	XHTML
<HR>	<hr />
<IMG SRC="dibujo.gif">	

Figura 2.14
Los elementos "vacíos" deben llevar terminación

- Todos los elementos deben estar anidados ordenadamente.

En HTML no hace falta tener especial cuidado en ordenar los anidamientos de las etiquetas (etiquetas dentro de otras etiquetas), siendo posible que existan solapamientos. Al igual que sucede con XML, en XHTML no se permiten tales libertades, debiendo tener especial cuidado en el orden en el que se realizan los anidamientos, y si una etiqueta de principio tiene el primer orden, otra el segundo y otra el tercero, por ejemplo, se deben situar las etiquetas de final de tal manera que primero se defina la del tercer orden después la del segundo y finalmente la del primero.

En la figura 2.15 se puede ver un ejemplo práctico sobre este punto.

HTML	XHTML
Este texto está en <I>cursiva <B>cursiva-negrita </I>negrita </B>y normal.<P>	Este texto está en cursiva cursiva-negrita negrita y normal.

Figura 2.15
Todos los elementos deben estar anidados ordenadamente

- Los valores de atributos iguales sin variantes no pueden ser simplificados.

Algunos atributos de HTML solo pueden tener un único valor, por lo que se permite "minimizarlos", o sea, dejar solo el atributo (o el valor, ya que son iguales).

Esto es corriente con los elementos <option>, <input> y <dl>, y así, es muy corriente encontrarnos con descripciones como <option value="valor" selected>, <input type="tipo" checked> o <dl compact>, cuando se tendrían que describir como <option value="valor" selected="selected">, <input type="tipo" checked="checked"> o <dl compact="compact">.

Según lo dicho, los ejemplos anteriores quedan en XHTML como se muestra en la figura 2.16.

HTML	XHTML
<OPTION VALUE="valor" SELECTED> <INPUT TYPE="tipo" CHECKED> <DL COMPACT>	<option value="valor" selected="selected"> <input type="tipo" checked="checked"> <dl compact="compact">

Figura 2.16
Los valores de atributos iguales sin variantes no pueden ser simplificados

- Existen elementos obligatorios.

A alguno le puede parecer un tanto quisquilloso este punto, pero en XHTML no se permite la ausencia de cualquiera de los elementos <head> y <body>.

También está regulado que <title> debe ser el primer elemento de la sección <head> ... </head>.

En la figura 2.17 se puede ver un ejemplo práctico sobre este punto.

HTML	XHTML
<HTML> <HEAD> <STYLE>...</STYLE> <TITLE>...</TITLE> </HEAD> </HTML>	<html> <head> <title>...</title> <style>...</style> </head> <body> ... </body> </html>

Figura 2.17
Existen elementos obligatorios

- Los documentos XHTML deben incluir una declaración de "tipo de documento".

Aunque esta norma ya existe en los documentos HTML, la verdad es que se utiliza en muy pocas ocasiones, siendo una novedad para muchos diseñadores web

El motivo de la necesidad de esta declaración es dejar bien claro que nuestro documento se ajusta a una determinada DTD, definida por el W3C como "una colección de declaraciones XML que define la estructura, los elementos y los atributos que es posible utilizar en un determinado documento". En otras palabras, una DTD es una descripción de las normas que nos indica qué cosas pueden hacerse en nuestro documento y qué cosas no pueden hacerse

La declaración de "tipo de documento" debe ser la primera línea de una página XHTML, delante incluso del elemento <html>.

Los documentos XHTML deben hacer referencia a una de las tres siguientes DTDs: Strict, Transitional o Frameset, siendo todas ellas unas aproximaciones, más o menos completas, a la especificación HTML 4. Sus formatos y características más importantes son:

- Strict:

  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

  Se utiliza cuando se da formato a los textos a través de CSS (Cascading Style Sheets), o sea, cuando no se recurre a las etiquetas <font> y <table> para controlar la forma en la que los navegadores muestran el contenido del documento.

- Transitional:

  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

  Se utiliza cuando no se describe la presentación de los documentos por medio de hojas de estilo en cascada, prefiriendo la descripción a base de etiquetas. Es el sistema adecuado para cuando se desea facilitar el acceso a usuarios con navegadores sin posibilidades de tratamiento de CSS.

- Frameset:

  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Frameset//EN" "http://www.w3.org/TR/xhtml1/DTD/frameset.dtd">

  Se utiliza cuando los documentos incorporan cuadros (frames).

Así pues, un ejemplo del código mínimo que habrá de tener un HTML es:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"  "DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
 <head>
  <title>Erase una vez</title>
 </head>
 <body>
  <p>Moved to <a href="http://vlib.org/">vlib.org</a>.</p>
 </body>
</html>
```

- El elemento raíz.

El elemento raíz de un documento XHTML debe ser siempre <html>. No puede existir nada antes de la etiqueta de principio <html> (salvo la declaración del tipo de documento). Tampoco se puede añadir nada después de la etiqueta de final </html>.

La etiqueta de principio <html> de un documento XHTML debe incluir un atributo que especifique el "espacio de nombre" (namespace) que utiliza el documento. El atributo es el mismo que se utiliza en XML, esto es: xmlns, siendo el valor de dicho atributo la palabra xhtml seguida del número 1 (uno).

Según el W3C, "un nombre de espacio XML es una colección de nombres, identificados por una referencia URI, que es utilizada en los documentos XML como tipos de documentos y nombres de atributos". Dicho más claro, el nombre de espacio XHTML es una lista con las etiquetas válidas que pueden ser utilizadas en un documento XHTML.

De acuerdo con lo dicho anteriormente, la etiqueta del elemento raíz será:

<html xmlns="http://www.w3.org/1999/xhtml">

- Elementos vacíos

Se ha de incluir un espacio entre / y > para los elementos vacíos, i.e.
, <hr /> and . Aunque también se tiene la sintaxis alternativa
</br>.

- Uso de Ampersands en los atributos

Cuando el valor de un atributo contenga un &, éste deberá sustituirse por su equivalente en caracteres (i.e. "&"). Por ejemplo, en el atributo href, la expresión:

http://my.site.dom/cgi-bin/myscript.pl?class=guest&name=user

sustituirá a la expresión:

http://my.site.dom/cgi-bin/myscript.pl?class=guest&name=user

- Los elementos <script> y <style>.

Si dentro del código HTML se describen elementos que incluyen listados en lenguajes diferentes del HTML, como ocurre con los elementos <script> o <style>, XHTML exige que se acoten los guiones en una sección CDATA. Las secciones CDATA ignoran el significado de los caracteres que incluyen, evitando problemas con entidades que puedan confundirse con las etiquetas del HTML, como ocurre con los delimitadores "<" y ">", por ejemplo

El único delimitador que no puede ser utilizado dentro de los guiones es "]]>", ya que es que utiliza la propia sección CDATA para saber dónde finaliza su función.

En la figura 2.18 se puede ver un ejemplo práctico sobre este punto.

HTML	XHTML
<SCRIPT LANGUAGE="JavaScript"> <!-- document.write("<P>Texto de prueba</P>"); //--> </SCRIPT>	<script language="JavaScript"> <!-- <![CDATA[document.write(" Texto de prueba ");]]> //--> </script>

Figura 2.18
Los elementos <script> y <style>

En muchos casos se puede evitar la utilización de las secciones CDATA, incluyendo los códigos en archivos externos y aplicando variantes similares a:

```
<script language="JavaScript" src="codigo.js"></script>
<link href="hoja_de_estilo.css" />
```

Con lo comentado en los temas anteriores habrá quedado clara la forma de conseguir que los nuevos proyectos HTML se ajusten a las normas del XHTML, e incluso que es relativamente fácil convertir antiguos documentos HTML en renovadas páginas web que sigan la normativa más reciente.

No obstante, existen documentos y herramientas que pueden facilitar enormemente la labor, sobre todo al principio, cuando surgen las primeras dudas.

La utilidad más importante para los interesados en el XHTML es la propia especificación XHTML 1.0 Specification, que se puede encontrar en el W3C.

En el website del W3C se encuentran disponibles las DTDs: Strict, Transitional y Frameset, que si se pueden referenciar desde cada documento XHTML, también es práctico tenerlo, tanto para estudiar su contenido, como para ser utilizado sin necesidad de conexión. Eso si, hay que asegurarse de que las DTDs que se tengan esten actualizadas.

2.7 Cascading Style Sheets (CSS)

CCS (Cascading Style Sheets: Hojas de estilo en cascada), es un conjunto de procedimientos que nos llevan a controlar distintos aspectos visuales y dinámicos de las páginas web, tales como fuentes, colores, márgenes y otros. Se constituye con un pequeño archivo que se vincula a una o más páginas, con el cual se consigue un aspecto similar para todas.

El término en cascada se utiliza debido a que más de una Hoja de Estilo puede afectar a la misma página web.

Las CSS contienen "reglas" para determinar la manera en que el estilo deseado debe ser aplicado a las páginas web. Para relacionar una página con un archivo CSS necesitamos en primer lugar un "selector", cada selector contiene "declaraciones" y las declaraciones tienen dos partes: propiedad y valor. CSS soporta 35 diferentes propiedades que pueden ser aplicadas a selectores a la hora de determinar la presentación de una página HTML.
Las propiedades incluyen "background", "font-size", "font-weight", "line-height", etc. Las reglas, entonces, están compuestas por la sumatoria de un selector y una declaración. Una regla puede usualmente presentarse de esta manera:

selector {propiedad :valor; propiedad :valor; }

Veamos un ejemplo para conseguir un párrafo pintado en verde:

P {color:green}

P - Es el selector y la regla (encerrada entre {} tiene una declaración)
color - Es la propiedad a la que se le va asignar un valor
green - Es el valor asignado; junto con la anterior propiedad constituye la declaración

2.8 Active Server Pages (ASP)

Cuando la World Wide Web irrumpió en la establecida escena de Internet a principios de los años 90 era un medio estático. Las páginas web no eran más que archivos de texto, si bien es cierto que era texto con un formato especial en HTML, no podía cambiar o adaptarse a la introducción de datos por parte del usuario o las condiciones actuales.

ASP (Active Server Pages: Páginas cuyo código se ejecuta del lado del Servidor de Aplicaciones Web) : Es una tecnología Web que permite crear páginas Web plenamente dinámicas e interactivas con el usuario.

Las ASPs contienen comandos de programación. La reducción en términos de complejidad es enorme. Y lo que es más, el lenguaje que se suele utilizar es VBScript, es mucho más sencillo que la mayoría; por lo que es más fácil que pueda utilizarlo una persona sin

muchos conocimientos de programación de sistemas, siendo muy corta la curva de aprendizaje, en ese sentido.

Al igual que HTML, las ASPs se pueden crear con un simple editor de texto, como el Block de Notas de Windows (Notepad) o vi de Unix, pero Microsoft tiene una herramienta que puede facilitar esta tarea, se llama Visual InterDev, forma parte de la Suite de productos Visual Studio, y la versión actual, 6.0, incluye los componentes en tiempo de diseño (DTC: Design Time Controls), que permiten automatizar el proceso de creación de páginas.

Microsoft® Active Server Pages (ASP) funciona de la siguiente manera:

Cuando el servidor de Web recibe una petición del contenido de alguna página ASP, este procesa scripts (código fuente dinámico para Web) que se ejecutan únicamente del lado del servidor y con base en ello, construyen la página que como respuesta a dicha petición, se visualiza en el navegador o browser (Internet Explorer, Netscape Navigator o algún otro de uso común entre la gente que navega en la Internet). Además de ello, los archivos ASP pueden contener código HTML (el cual a su vez puede incluir scripts que se ejecutan del lado del cliente), así como llamadas a componentes COM que ejecutan una gran variedad de tareas, como puede ser el conectarse a una base de datos o procesar lógica de negocios.

Los scripts generados con ASP, se ejecutan del lado del servidor de Web, por tanto, este código no puede copiarse ya que los usuarios únicamente verán el código que resulta como producto final de esa ejecución de código del lado del servidor de Web y que no es más que una página Web en HTML ya generada con ASP, lo anterior brinda protección al autor de las páginas ASP, como protección contra los llamados Hackers o piratas de la información.

Una de las características que hacen que ASP presente funcionalidad es que permite el Acceso a Datos almacenados en Bases de Datos, preferentemente relacionales, esto como sigue:

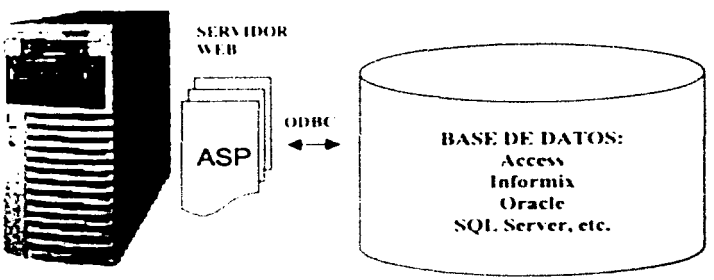


Figura 2.19
Acceso a Datos con ASP

Como puede apreciarse en la figura 2.19, todas las Bases de Datos tienen una interfaz de programación de aplicaciones (Application Programming Interface, API) que permite a los programadores comunicarse con ellas, utilizando ya sea Visual InterDev de Microsoft o alguna otra herramienta de desarrollo de Sistemas con Comunicación con Bases de Datos relacionales.

ODBC (Open Database Connectivity: Conectividad con Bases de Datos bajo tecnología abierta) actúa de traductor. Los programadores pueden escribir en la API de ODBC y ODBC traduce dichos comandos para la base de datos especifica utilizando un controlador que es especifico de la misma. De esa forma, las aplicaciones trabajan siempre que esté instalado el controlador apropiado.

ASP evita que tenga que se tenga que elegir, a la hora del desarrollo de las aplicaciones una base de datos en particular, pues utiliza un controlador ODBC estándar para comunicarse con ella.

Bajo este esquema, se debe contar con un Servidor de Web que soporte ASP, con un Servidor de Base de Datos (Access, ORACLE, Informix, SQL Server o algún otro, según las necesidades de negocios del cliente para el cual se desarrolle el Sistema con ASP) que se comunique con el Servidor de Web vía ODBC. Tras conectar ASP con una Base de Datos, hay muy poca o ninguna diferencia en la forma en que se accede a ella desde las páginas.

2.9 DLL (Data Link Library: Biblioteca de enlace de datos)

Una DLL es un tipo de componente ActiveX, el cual contiene código ejecutable, tal como un .exe o un .ocx.

Un componente ActiveX, bautizado así por Microsoft, contiene código que puede ser utilizado por otras aplicaciones.

Existen 3 tipos de componentes ActiveX que pueden crearse, en nuestro caso, con Visual Basic: estos son los controles ActiveX, documentos ActiveX y componentes con código ActiveX.

Controles ActiveX: Se les conoce formalmente como controles OLE (Object Linking Embedding, en idioma inglés); son elementos de tipo estándar para la creación de interfases de usuario que permiten reutilizar formas y cajas de diálogo con otras aplicaciones.

Documentos ActiveX: Se les conoce formalmente como objetos de tipo documento y son componentes que deben alojarse y activarse en una aplicación cliente. La tecnología de documentos ActiveX es una extensión de los documentos OLE. Incluye objetos de edición visuales, objetos a incrustar en aplicaciones, así como aplicaciones que incluyen comandos

del Sistema operativo, tales como Internet Explorer, pasando por diferentes tipos de documentos.

Componentes con código ActiveX: Formalmente conocidos como Servidores OLE; son bibliotecas de objetos. Las aplicaciones cliente utilizan componentes con código ActiveX, mediante la creación de objetos a partir de clases que el mismo componente incluye. El cliente hace llamadas a las propiedades, métodos y eventos propios del objeto.

Cualquier aplicación que soporte la Automatización estándar, puede utilizar componentes con código ActiveX, los cuales se programan por lo general con Visual Basic de Microsoft. Incluyen interacción con el mismo Visual Basic, Excel, Access, Project, Visual FoxPro y Visual C++.

Visual Basic se encarga de toda la complejidad involucrada en la creación de componentes con código ActiveX, como lo es la creación de bibliotecas de tipos de objetos y el registro de los componentes, de manera automática.

Así pues, una DLL es la reunión de procedimientos y funciones encapsulados en forma de componente, que tienen varias ventajas, entre otras:

- Al programar una DLL se puede contar con todo el poder de programación de Visual Basic.
- Se pueden mover o sustituir fácilmente, es decir, el mantenimiento es relativamente fácil.
- Una misma DLL se puede utilizar para varios clientes.
- Existe la compatibilidad binaria, lo cual facilita su mantenimiento.
- Una DLL es relocalizable, lo cual facilita de igual forma, su mantenimiento.
- Una DLL es multilenguaje, de hecho la DLL utilizada en nuestro sistema, fue desarrollada en Visual Basic.
- Una DLL se compila por separado de la aplicación.
- Finalmente, dado que una DLL es encapsulada, los componentes no muestran cual fue el lenguaje de programación que se utilizó en su desarrollo.

Capítulo 3

DESARROLLO DEL SISTEMA

Hoy en día casi todas las instituciones y empresas cuentan con algún tipo de sistema de control e identificación de personal, unos muy simples que van desde una tarjeta de identificación o una clave con contraseña, los circuitos cerrados y en menor escala sistemas más sofisticados como lo son las tarjetas magnéticas, dispositivos con código de barras y los sistemas biométricos que reconocen voz, huellas digitales, retina

Aunado a estas tecnologías, los sistemas informáticos se han desarrollado a gran nivel, permitiendo innovar en casi cualquier campo, pero sobre todo enfocándose cada vez más a lo que parece un futuro inminente, el uso generalizado de Internet.

Dado que a finales de la década de los noventas, Internet se convirtió en una herramienta de gran ayuda en lo que a difusión y distribución masiva de información se refiere, hoy podemos ver que en gran medida, la tendencia de los sistemas, es trabajar bajo una plataforma orientada al entorno Web.

Es por eso que se desarrolló el Sistema de Identificación y Control de Acceso de Personal en Línea, un prototipo para las diferentes áreas que integran un centro de trabajo, con el fin de contar con un registro cuantificable de personal así como su autenticación.

3.1 Planteamiento

Cuando en un centro de trabajo el control de accesos e identificación de personal se vuelve complicado, pueden existen varias razones por la cual no se esta cumpliendo con su meta, como puede ser que las instalaciones son relativamente amplias y el personal poco, una mala distribución de los módulos de monitoreo, los cuales, debido a su poca comunicación no mantienen el nivel de control tan óptimo como se requiera. Ahora bien, si existe la necesidad de supervisar al personal que tiene ciertas responsabilidades vitales dentro de la empresa o institución, sin estar presente, o bien, recabar información general relacionada a la identificación del personal como:

- Asegurarse que el personal de seguridad recorre las instalaciones durante el transcurso de la noche.
- Si se encuentra personal no autorizado en áreas restringidas de la empresa.
- Localizar a personal dentro de la empresa.
- Realizar estadísticas del personal relacionadas con los accesos al centro de trabajo.

Es por eso que para este proyecto se delimito nuestro centro de trabajo de la siguiente forma: Contamos con una instalación que se divide en 3 secciones, llamaremos secciones a cada una de nuestras áreas de trabajo y que existirán tantas, como áreas se tengan. En la figura 3.1 se muestra un esquema de nuestro centro de trabajo propuesto.

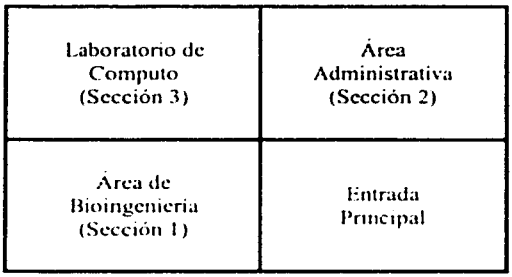


Figura 3.1
Esquema del Centro de Trabajo

Para cada una de nuestras secciones, se asigna un grupo de personas. Estos grupo tienen políticas para su sección y no se les bloquea el acceso a las demás secciones, pero estos accesos deben de quedar registrados. Dentro de nuestras políticas del centro de trabajo debemos de tener en cuenta las siguiente limitantes :

- Una persona no puede entrar a una sección si no tiene permiso para ingresar a ella.
- Una persona puede entrar o salir de cualquier sección **si y sólo si** antes entró por la puerta principal.
- Una persona no puede entrar o salir del edificio si ya antes entró a su sección y aún no ha salido de ella.
- Los visitantes pueden entrar o salir de la sección que le corresponde **si y sólo si** antes entró por la puerta principal.

Además de estas características, el sistema proporciona información adicional en cualquier momento del personal como puede ser de su asistencia, de su hora de entrada, de su hora de salida. Esta información esta disponible solamente para un determinado grupo de personas, que desde cualquier lugar donde se encuentren, pueden acceder a ella.

Por eso el sistema debe de:

- Ser un sistema para WEB
- Contar con al menos 2 zonas de acceso.
- Contar con delimitaciones para usuarios
- Fácil de instalar y de dar mantenimiento
- Amigable y contar con una interfaz grafica

3.2 Análisis

Necesitamos primero definir cual será el sistema de identificación a usar para posteriormente dar un modelo del sistema.

Para el desarrollo del sistema se han analizado diferentes dispositivos de identificación como lo son:

- Claves y contraseñas
- Códigos de barra
- Tarjetas magnéticas
- Sistemas biométricos

Se han descrito sus características, sus ventajas y sus desventajas, todas ellas desde un punto de vista técnico, ahora bien económicamente hablando, el sistema de más bajo costo para su desarrollo y colocación es el de claves y contraseñas;

Ahora bien si consideramos los sistema biométricos, en la siguiente tabla se podrá observar alguna características especiales así como los costos de cada uno de ellos.

Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación y/o autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas	Artritis, reumatismo	Firmas fáciles o cambiantes	Ruido, resfriados
Utilización	Instalaciones nucleares, servicios médicos centros penitenciarios	Instalaciones nucleares, servicios médicos, centros penitenciarios	Policía, industrial	General	Industrial	Accesos remotos en bancos o bases de datos
Precio por nodo (USD)	5000	5000	1200	2100	1000	1200

Tabla 1 Comparación de métodos biométricos

Para los dispositivos lectores de códigos de barras se encontraron que los precios oscilaban desde los $1,000.00 MN hasta $10,000.00 MN, dependiendo del tipo y modelo del lector, por ejemplo:

Spark LS 1006 $ 2,500.00 M.N.

HotShot LS 2100 $4,200.00 M.N.

Se tomo la decisión de seleccionar a los códigos de barra como el sistema de identificación más viable por las siguientes razones:

- Bajo costo.
- Facilidad de trabajo.
- Facilidad de integración con el software desarrollado.

Además de trabajar con los códigos de barras, nos apoyaremos en las claves y contraseñas, como un medio más dentro del sistema.

Como ya se ha mencionado los códigos de barras tienen diferentes simbologías, dentro de las más comunes tenemos:

- UPC
- Código 39
- Código 128
- Codabar
- MSI-Plessey
- PDF417

El Código 39 (Código 3 de 9) es la simbología más popular para identificaciones, inventarios y cuando se tiene la necesidad de rastrear algo. Tiene una longitud variable, permite cadenas alfanuméricas y puede ser impreso en varios tamaños y proporciones. Este es el código de barras que se usa en negocios de arrendamiento de videos, en etiquetas de identificación y en cualquier lugar donde simplemente se necesita un código de barras. La versión completa de ASCII admite los primeros 128 caracteres. Algunas veces se usa con un dígito de verificación optativo.

Figura 3.2
Código 39

Debido a que el sistema tendrá un código de usuario y una contraseña de acceso en caracteres alfanumérico (0-9 y de A a la Z), se decidió utilizar el Código 39, ya que incluye dígitos 0-9, letras de la A-Z (solo mayúsculas), el dígito verificador es opcional y cuenta con una longitud variable (recomendable hasta 25 caracteres) estas características son ideales para códigos de usuario y claves de acceso.

Estas es una tabla que resume las características del código.

CARACTERISTICAS	ALFANUMERICO
Juego de caracteres	10 números (0...9) 26 letras (A...Z) 7 Signos (-, ., *, $, /, +, %) El símbolo * siempre es el carácter Inicio/Fin
Composición del carácter	5 Barras Y 4 espacios 9 elementos de los que 3 deben de ser anchos.
Control	Posibilidad de dígito de control
Longitud	Variable
Ventajas	Código alfanumérico integral
Inconvenientes	Espacio necesario amplio
Sectores donde se aplica	Industria, Transporte, Comercio,

Es decir que para las entradas de cada sección se tendría lo siguiente:

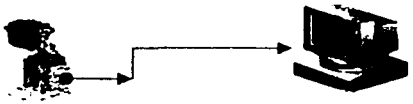


Figura 3.3
Lector de códigos de barras conectado a una PC

Ahora si hablamos de tres secciones y una entrada principal nuestro esquema tendría un sistema como el mostrado en la figura 3.4

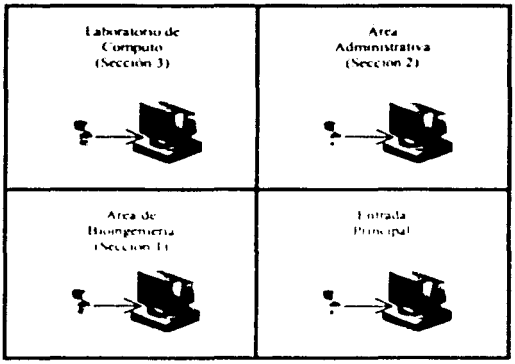


Figura 3.4
Esquema con los dispositivos de identificación

Como se necesita tener un registro de todos los movimientos que se dan en el centro de trabajo, es necesario tener una base de datos para poder almacenar esta información, pero no es posible tener una base de datos para cada una de nuestras secciones, por lo tanto es necesario instalar una red en el Centro de trabajo.

Para este centro en particular, se implementa una red Ethernet, con un Hub o Switch junto con un servidor para la base de datos. En la Figura 3.5 se muestra el diseño de la red.

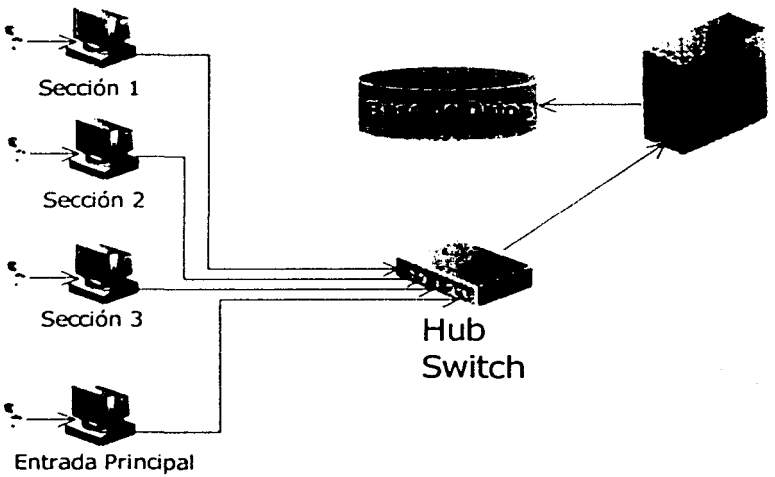


Figura 3.5
Diseño de la red

Además, se contara con una computadora que será la **Estación de monitoreo**, ésta en un momento dado, podrían ser opcional ya que, cualquiera de las computadoras que funcionan con entradas, podría funcionar como **Estación de monitoreo**. También, es posible habilitar una Estación remota de identificación, que estaría conectada a nuestra red través de Internet.

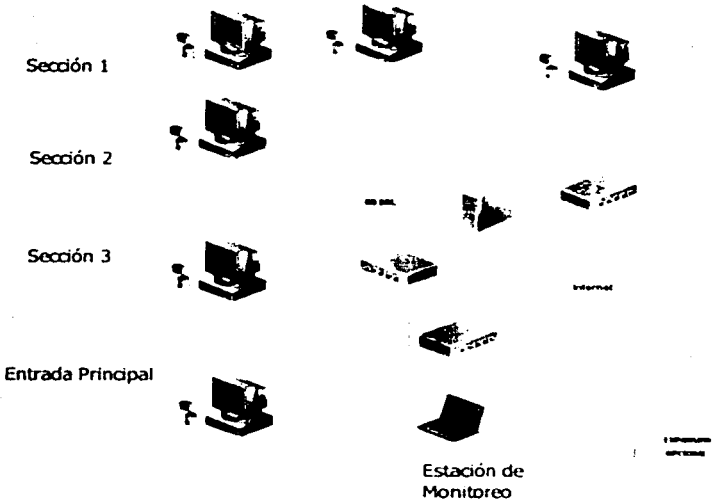


Figura 3.6
Diseño del sistema con expansión e internet

3.3 Características

Para el desarrollo del sistema se deben de considerar las siguientes características:

- Un servidor WEB.
- Una aplicación que nos permita enlazar las diferentes terminales con nuestro servidor de Web.
- Una Base de Datos Relacional.
- Comunicación permanente entre terminales vía TCP/IP.

Especificaciones del SERVIDOR que contendrá el sitio WEB y la Base de Datos Relacional:

- Requerimientos de Software:

  NT 4.0 con Service Pack 4 o superior o Windows 2000 Server.
  Internet Explorer 5.0 o superior.
  Microsoft MSXML 3, que es el parser de XML.

Microsoft ActiveX Data Objects 2.5 o superior, el cual nos provee de las herramientas para las operaciones básicas de Bases de Datos: obtener, examinar, editar y actualizar datos.
Microsoft Transaction Server.
Microsoft SQL Server 7.0.
Internet Information Services 3.0 o superior.
Dundas Upload versión 2.0, que es un dll ActiveX gratuito, el cual nos sirve para subir archivos remotamente al servidor.

- Requerimientos de Hardware:

  500 MB libres mínimo de espacio en disco duro.
  128MB en RAM.
  Procesador Pentium III a 500MHz o superior.
  CD ROM

3.4 Diseño del Programa

Para poder realizar el programa para que pueda ser una aplicación WEB se has recurrido a las siguientes tecnologías como lo son ASP, HTML, XSL. Los archivos GIF y JPG corresponden a imágenes variadas del sitio, mientras que los demás archivos constituyen el núcleo del código principal del sistema.

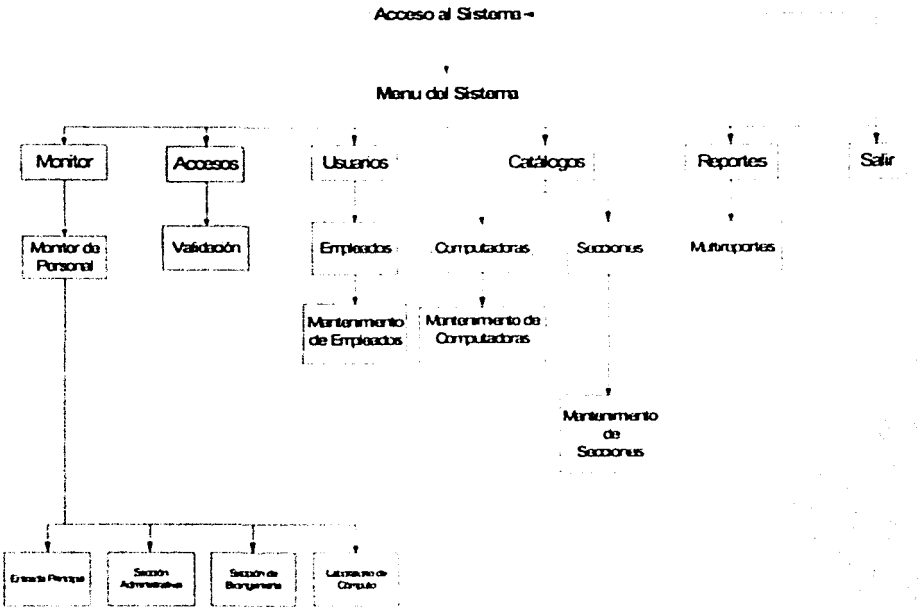


Figura 3.4
Modelo propuesto para el mapa de navegación

Este el modelo del sitio propuesto, cada uno de los recuadros es una página que a su vez se conectan a otra.

3.4.1 Bosquejo de las pantallas

El sitio virtual se llamará Monitor, por lo cual deberemos teclear en nuestro Explorador de Internet, la siguiente dirección URL http monitorunam prodigyweb net mx

De entrada aparecerá una pantalla con un recuadro central, en la cual, debemos proporcionar nuestra clave (user id) y contraseña (password).

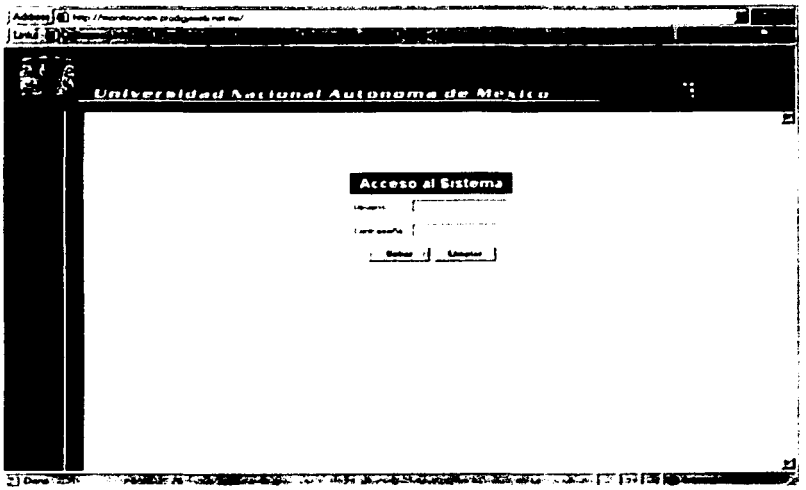


Figura 3.5

Existirán tres perfiles básicos:

- Administrador. Tendrá permiso a todos los menús del sistema.
- Monitor. Tendrá permiso sólo al menú de búsqueda de usuarios del sistema.
- Usuario y Visitante. Es el que funciona exclusivamente para entradas y salidas del personal.

Asi pues, se desplegarán menús y pantallas personalizados, en función de los permisos otorgados a cada usuario, de acuerdo a los perfiles antes mencionados. En la Figura 3.6 se muestra el menú del usuario administrador

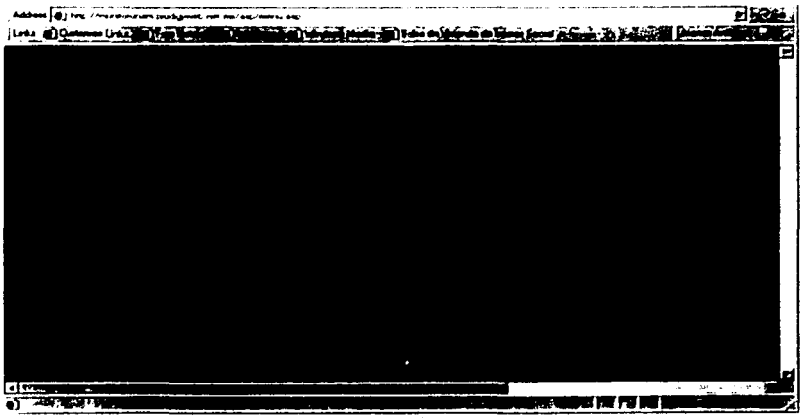


Figura 3.6

A continuación se bosquejan los menús y submenús del sistema:

Menú Monitor de personal. Este menú servirá para monitorear al personal que se encuentre en las diferentes secciones del inmueble.

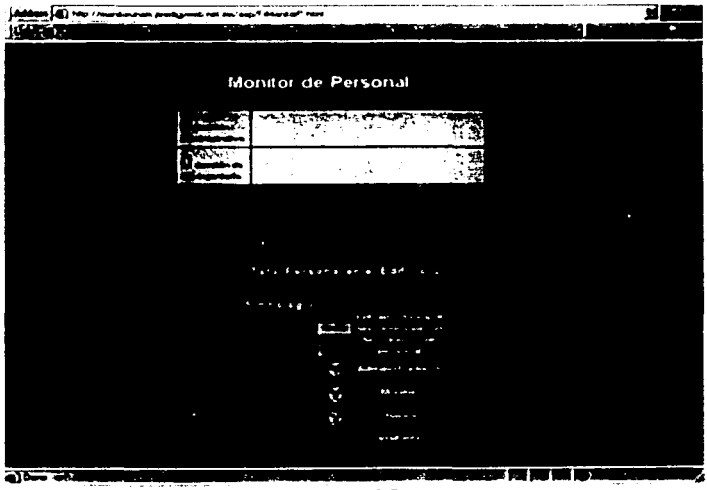


Figura 3.7

Menú Accesos del personal. Es el menú que contendrá una pantalla con un recuadro donde se leerán las credenciales del personal. Esta es la pantalla a la que tendrán acceso el personal con perfil de USUARIO, la cual les permitirá pasar sus códigos de barra y así acceder o no a sus secciones respectivas.

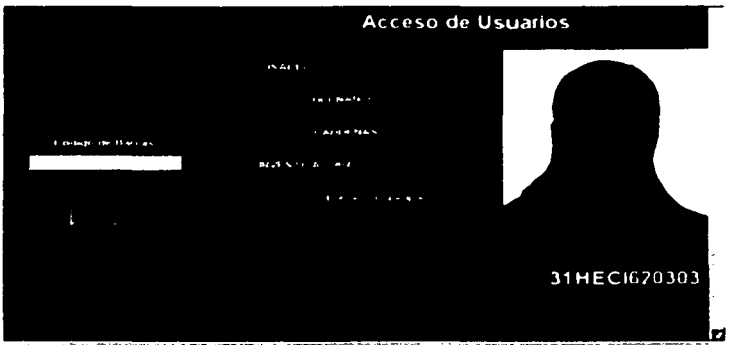


Figura 3.8

Menú Usuarios. Este menú servirá para ver la base de datos de los empleados con la opción dar de alta al usuario. Entre los datos más representativos que se capturarán son: el nombre completo, teléfono, sección en donde trabaja, clave de usuario, contraseña del usuario, fotografía, correo electrónico, jerarquía del usuario.

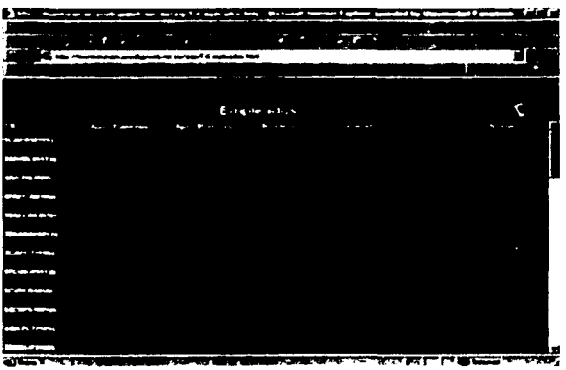


Figura 3.9

Figura 3.10

Menú Catálogos. En este menú se dará mantenimiento a los diversos catálogos del sistema. Contiene dos submenús: el catálogo de Computadoras y el de Secciones.

Figura 3.11

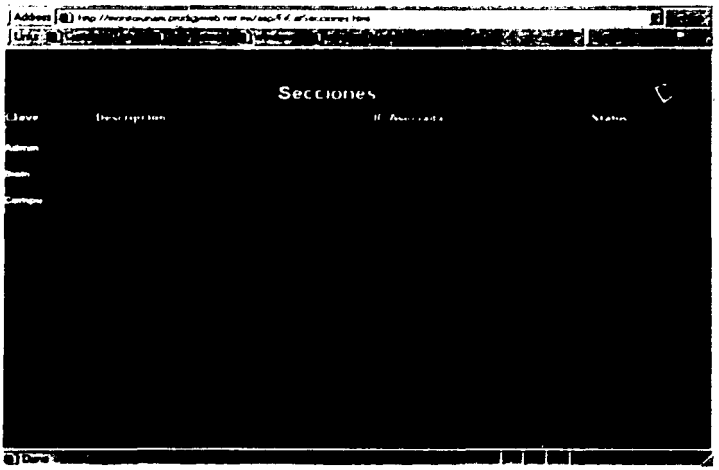


Figura 3.12

El primer catálogo (Figura 3.11) es donde se captura la información descriptiva de las computadoras cliente que tienen asignado un lector CB y su correspondiente sección. Dentro de la información más descriptiva está la IP de la máquina para poder rastrear de dónde vino la petición de apertura de puertas.

El segundo catálogo (Figura 3.12) es donde se captura la información de las secciones laborables. También se registra la relación entre la sección y la IP de la máquina que estará asociada a esa sección.

Menú Reportes. Este menú contiene a los reportes de personal por sección y reporte de personal por fecha. Los reportes generarán un informe del personal laboral presente o no presente con los criterios de búsqueda por rango de fechas y/o sección laboral (Figura 3.13).

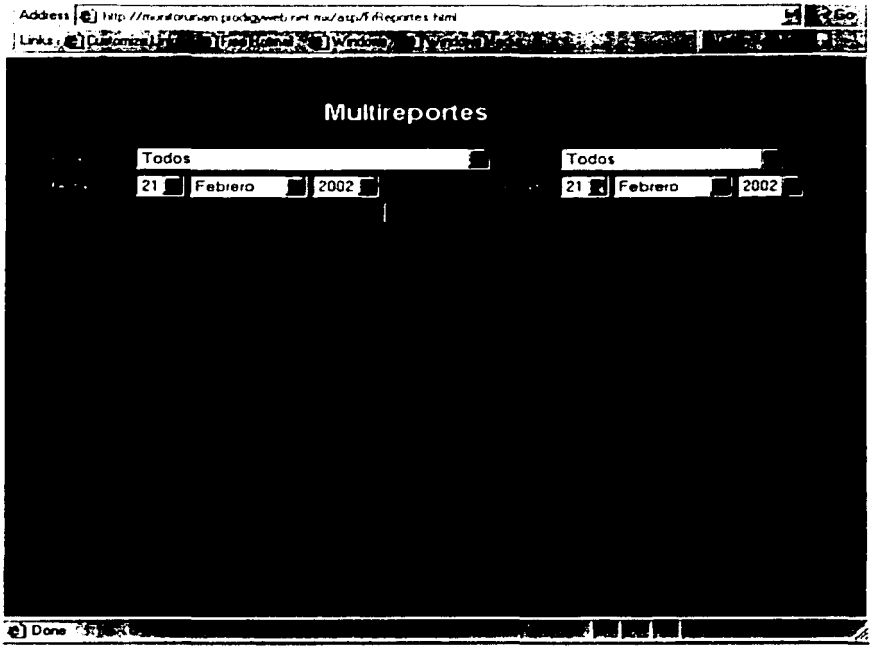


Figura 3.13

3.4.2 Base de Datos

Para el Sistema de identificación y control de acceso de personal en línea, fue necesario implementar una Base de Datos del tipo Relacional, ya que a raíz del análisis y la problemática en este caso se tiene lo siguiente:

- **Planteamiento de la Base de Datos:**

  Se requiere implementar una Base de Datos que nos permita:

  - Almacenar, mantener y recuperar datos referentes a cada usuario que acceda al "Sistema de identificación y control de acceso de personal en línea".

  - Almacenar, mantener y recuperar información referente a opciones y subopciones de un Menú de opciones a través de las cuales los usuarios podrán interactuar con el Sistema.

- Almacenar, mantener y recuperar información referente a un Histórico de accesos al Sistema por parte de los usuarios y de las personas que accedan a una sección dentro de un Centro de trabajo.

- Almacenar, mantener y recuperar información referente a Computadoras Personales (PCs) que estarán intercomunicadas a través del protocolo de comunicaciones TCP/IP, valiéndonos de una dirección IP asociada a cada PC.

- Almacenar, mantener y recuperar información referente a secciones dentro de un Centro de trabajo.

- Almacenar, mantener y recuperar información referente a Grupos a los cuales pertenece un usuario.

- Almacenar, mantener y recuperar información referente a Grupos asociados a las diferentes opciones del Menú.

- Por último, se requiere almacenar intentos fallidos de acceso a una sección del Centro de trabajo.

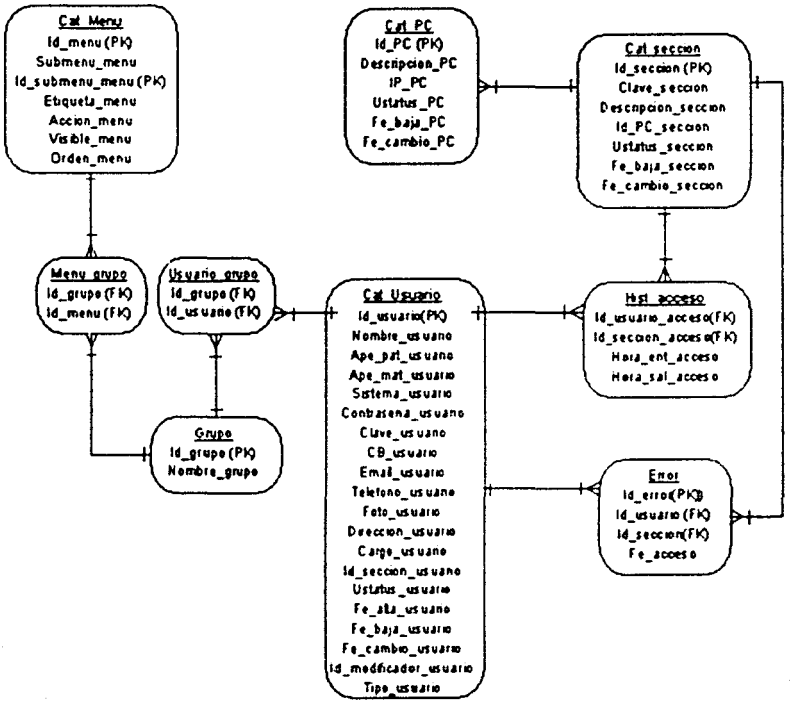
• Entidades:

- Catálogo de usuarios.
- Catálogo de menús.
- Histórico de accesos.
- Catálogo de Computadoras Personales.
- Catálogo de secciones.
- Catálogo de Grupos.
- Tabla relación de Usuarios con Grupos.
- Tabla relación de Catálogo de Menús y Grupos.
- Tabla para almacenar Errores referentes a intentos de acceso fallidos por parte de visitantes.

• Atributos por entidad:

- **Ver Diccionario de Datos anexo 1.**

- **Diagrama Entidad - Relación:**



- **Relaciones:**

Del Diagrama Entidad – Relación, tenemos:

- Que a un identificador de usuario corresponde uno ó más Grupos.
- Que a un identificador de usuario corresponde uno ó más Históricos de accesos a una sección del Centro de trabajo.

- Que a un identificador de usuario corresponde uno ó más intentos fallidos de acceso, en lo que respecta a los visitantes que ingresan al Centro de trabajo.
- Que a un identificador de sección corresponde una ó más direcciones IP asociadas a una ó más Computadoras Personales (PCs).
- Que a cada opción del Menú corresponde una ó más subopciones del mismo.
- Que a cada opción del Menú corresponde uno ó más Grupos.
- Que a cada Grupo corresponde una ó más opciones del Menú.
- Que existe un solo tipo de usuario para cada identificador de usuario.
- Que cada identificador de usuario presenta un solo estatus de usuario.
- Que cada PC tiene un solo estatus asociado (Activo o Inactivo).
- Que cada usuario tiene un Código de Barras asociado a su identificador de usuario.
- Que cada usuario tiene una Clave de usuario asociada a su identificador de usuario.
- Que cada usuario tiene una Contraseña asociada a su identificador de usuario.

Capítulo 4

EVALUACIÓN DEL SISTEMA

4.1 Pruebas al Sistema utilizando conexión a Internet vía una Red LAN:

Las siguientes pruebas fueron realizadas sobre Internet con una distancia física entre el Cliente y el Servidor de aproximadamente 200 Km, teniendo como velocidades de salida hacia Internet para el Servidor 10Mbps y para el Cliente 2Mbps.

Prueba de registro de ingreso

Se realizaron pruebas con 20 usuarios registrados en el Sistema.
La primera prueba consistió en registrar el ingreso de 20 usuarios por la entrada principal, como se muestra la figura 4.1.

Resultados:

El tiempo de respuesta entre el registro del ingreso de usuarios fue de 1 segundo.

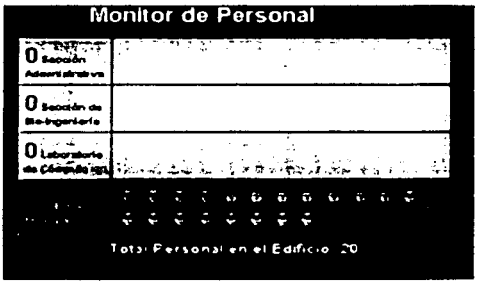


Figura 4.1.
Ingreso de 20 usuarios por la entrada principal.

Posteriormente estos usuarios fueron registrados 10 en la sección administrativa y 10 en la sección del laboratorio de cómputo (Figura 4.2).

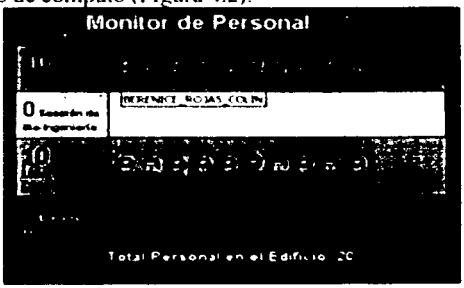


Figura 4.2.
Ingreso de 10 usuarios en la sección administrativa y de otros 10 en la sección del laboratorio de cómputo.

El siguiente paso realizado consistió en registrar las salidas del laboratorio de cómputo, la figura 4.3 muestra el monitoreo realizado después del registro de salidas.

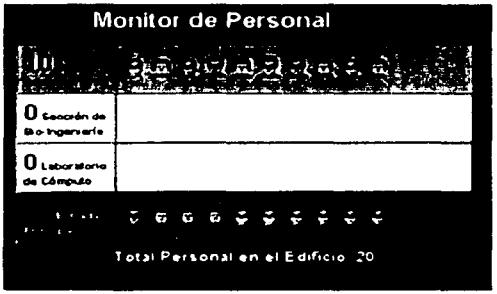


Figura 4.3.
Salida de 10 usuarios del laboratorio de cómputo.

Prueba de Alta de empleados

La prueba consistió en dar de alta a 50 usuarios con diferentes jerarquías.

Resultados:

Cuando la Clave de usuario ya estaba dada de alta, el Sistema mostraba el mensaje de la Figura 4.4, en este caso fue necesario regresar a la página anterior para poder dar de alta a ese usuario con otra Clave; en caso contrario, cuando la Clave no existía, el alta se realizó sin problema alguno.

Lo anterior garantiza la no duplicidad de Claves de usuarios dados de alta en el Sistema.

El tiempo de respuesta del sistema para esta prueba fue de 3 segundos.

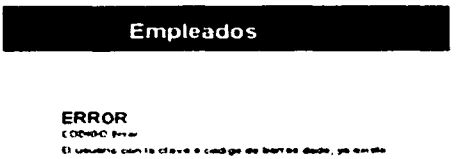


Figura 4.4. Mensaje de error generado al intentar dar de alta un usuario ya existente.

Prueba de tiempo de respuesta del monitoreo

Esta prueba consistió en tomar el tiempo que la página de monitoreo tarda en desplegar los datos de los accesos registrados en el Sistema de las diferentes Secciones del Edificio.

Tomando en cuenta que el Sistema hace un refresco automático de la pantalla cada 15 segundos y después muestra los datos del monitoreo, el tiempo de respuesta de la página de monitoreo fue de 1 segundo.

Pruebas de tiempo de respuesta de reportes

Caso I:

Se generó un reporte mediante el Sistema que incluyera a todos los usuarios en todas las secciones, en un periodo comprendido entre el 1 de Febrero del 2002 y el 22 de Febrero del mismo año (Figura 4.5).

Figura 4.5.
Reporte generado para todas las secciones, en un periodo del 1 al 22 de Febrero del 2002 para evaluar tiempo de respuesta.

Resultados:

El tiempo de respuesta del Sistema fue de 16 segundos, conteniendo 264 registros en el reporte.

Caso II:

Para un reporte para todos los usuarios y todas las secciones, con un periodo comprendido entre el 21 de Febrero de 2002 y el 22 de Febrero del 2002.

Resultados:

Se obtuvo un tiempo de respuesta de 12 segundos y un total de 166 registros en el reporte.

Caso III:

Para una reporte para todos los usuarios y todas las secciones con un periodo comprendido entre el 18 de Febrero de 2002 y el 20 de Febrero del 2002.

Resultados:

Se obtuvo un tiempo de respuesta de 3 segundos y un total de 33 registros en el reporte.

4.2 Pruebas al Sistema utilizando conexión a Internet vía MODEM:

Las siguientes pruebas fueron realizadas sobre Internet con una distancia física entre el Cliente y el Servidor de aproximadamente 300 km., teniendo como velocidades de salida hacia Internet para el Servidor 10Mbps y para el Cliente 48kbps.

Prueba de registro de ingreso

Se realizaron pruebas con 20 usuarios registrados en el Sistema.

La primera prueba consistió en registrar el ingreso de 20 usuarios por la entrada principal, como se muestra en la figura 4.6.

Resultados:

El tiempo de respuesta entre el registro del ingreso de usuarios fue de 2 segundos.

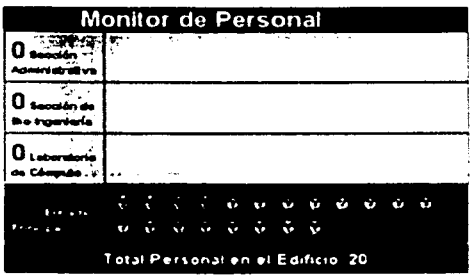


Figura 4.6.
Ingreso de 20 usuarios por la entrada principal.

Posteriormente estos usuarios fueron registrados 10 en la seccion administrativa y 10 en la sección del laboratorio de cómputo (Figura 4.7)

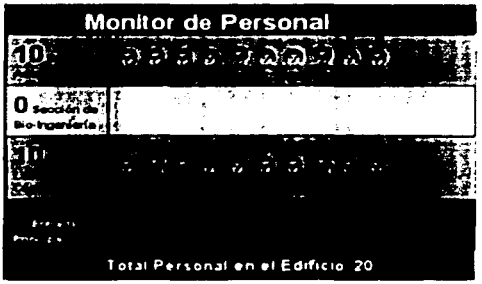


Figura 4.7. Ingreso de 10 usuarios en la sección administrativa y de otros 10 en la sección del laboratorio de cómputo.

El siguiente paso realizado consistió en registrar las salidas del laboratorio de cómputo, la Figura 4.8 muestra el monitoreo realizado después del registro de salidas.

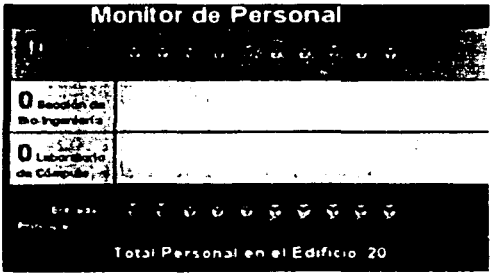


Figura 4.8.
Salida de 10 usuarios del laboratorio de cómputo.

Prueba de Alta de empleados

La prueba consistió en dar de alta a 50 usuarios con diferentes jerarquías.

Resultados:

Cuando la Clave de usuario ya estaba dada de alta, el Sistema mostraba el mensaje de la Figura 4.9, en este caso fue necesario regresar a la página anterior para poder dar de alta a ese usuario con otra Clave; en caso contrario, cuando la Clave no existía, el alta se realizó sin problema alguno.

Lo anterior garantiza la no duplicidad de Claves de usuarios dados de alta en el Sistema.

El tiempo de respuesta del sistema para esta prueba fue de 5 segundos

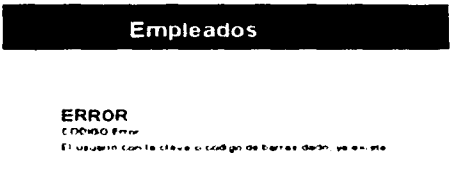


Figura 4.9.
Mensaje de error generado al intentar dar de alta un usuario ya existente.

Prueba de tiempo de respuesta del monitoreo

Esta prueba consistió en tomar el tiempo que la página de monitoreo tarda en desplegar los datos de los accesos registrados en el Sistema de las diferentes Secciones del Edificio

Tomando en cuenta que el Sistema hace un refresco automático de la pantalla cada 15 segundos y después muestra los datos del monitoreo, el tiempo de respuesta de la página de monitoreo fue de 2 segundos.

Pruebas de tiempo de respuesta de reportes

Caso I:

Se generó un reporte mediante el Sistema que incluyera a todos los usuarios en todas las secciones, en un periodo comprendido entre el 1 de Febrero del 2002 y el 22 de Febrero del mismo año (Figura 4.10).

Figura 4.10.
Reporte generado para todas las secciones, en un periodo del 1 al 22 de Febrero del 2002 para evaluar tiempo de respuesta.

Resultados:

El tiempo de respuesta del Sistema fue de 40 segundos, conteniendo 264 registros en el reporte.

Caso II:

Para un reporte para todos los usuarios y todas las secciones, con un periodo comprendido entre el 21 de Febrero de 2002 y el 22 de Febrero del 2002.

Resultados:

Se obtuvo un tiempo de respuesta de 25 segundos y un total de 166 registros en el reporte.

Caso III:

Para una reporte para todos los usuarios y todas las secciones con un periodo comprendido entre el 18 de Febrero de 2002 y el 20 de Febrero del 2002.

Resultados:

Se obtuvo un tiempo de respuesta de 11 segundos y un total de 33 registros en el reporte.

4.3 Pruebas de ruptura de ligas en el Sitio Monitor 1.0:

Estas pruebas se realizaron utilizando el software CyberSpyder Link Test Version 2.1.13.

Prueba Monitor 1.0
Resumen del resultado de la prueba

Prueba Iniciada: 2/21/2002 3:01:26 PM
Prueba Finalizada: 2/21/2002 3:01:27 PM
Tiempo transcurrido: 1 minuto con 4 segundos

Configuración
Tiempo de espera en la conexión: 30 segundos
Tiempo de respuesta: 30 segundos
Número de Intentos: 2
No existe limite de velocidad de respuesta

URL de inicio
http://monitorunam.prodigyweb.net.mx

Total de ligas checadas: 18
18 Ligas adecuadas

Existen 2 mensajes de precaución
Existen 8 URLS únicos
El sitio contiene 34 páginas HTML

Preparado: 2/21/2002 3:01:30 PM

Pruebas realizadas con:

CyberSpyder Link Test
Version 2.1.13

Prueba Monitor 1.0

Mensaje de Precaución – Organizado por Pagina URL

Este reporte contiene 2 items.
http://monitorunam.prodigyweb.net.mx/ (Monitor 1.0)

- Mensaje de precaución: 3004 El documento contiene mas de una etiqueta </body> o </frameset>!
- Mensaje de precaución: 3004 El documento contiene mas de una etiqueta </body> o </frameset>!
- Bottom of Form

Preparado: 2/21/2002 3:02:05 PM

Capítulo 5

MANUALES DE OPERACIÓN

Manual de Administración del Sistema de Identificación y Control de Acceso de Personal en Línea

El presente manual ayuda en la instalación y configuración del Sistema de Identificación y Control de Acceso de Personal en Línea. Está orientado a los Administradores de red.

Para cualquier duda relacionada con el funcionamiento del presente Sistema, se debe referirse al Manual de usuario.

Requerimientos:

- Microsoft Windows 2000 Server .
- Equipo compatible con Pentium a 133 MHz o superior.
- Se recomienda un mínimo de 256 MB de memoria RAM (el mínimo admitido son 128 MB y 4 GB el máximo).
- 1.0 GB de espacio libre en el disco duro. Se requiere espacio libre adicional del disco duro para el Servidor de Base de Datos (SQL Server 7.0 o superior).
- Unidad de CD-ROM.
- Monitor VGA o de mayor resolución.

Contenido del CD de instalación:

- DLL para llamadas a funciones y procedimientos propios del "Sistema de identificación y control de acceso de personal en línea".

- Archivos ASPs, CSSs, XSLs, includes, Jscripts y archivos de imágenes que permiten la interacción del usuario con el Sistema.

- Archivos de script para creación de Base de Datos, Tablas y usuarios para la comunicación del Sistema con SQL Server 7.0 o superior.

- El componente Dundas (para subir las fotos de los usuarios del Sistema que se registren en él, al servidor en el momento de generar su credencial para su autenticación).

- Los componentes para lectura y generación de Código de Barras.

- El Parser de XML, el cual es el intérprete de código XML útil en la personalización de Menús de opciones en el Sistema.

- **Habilitación de servicios de Internet.**

Se requiere habilitar los servicios del Internet Information Services (IIS).

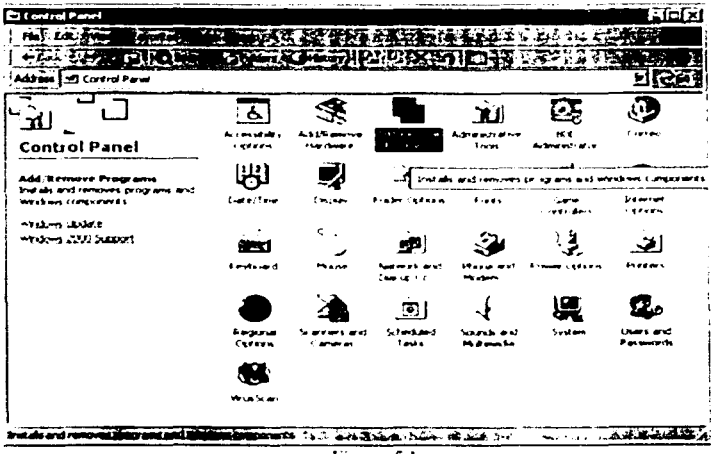


Figura 5.1
Desde el Panel de control es posible habilitar los servicios de Internet

Para ello, como se muestra en la Figura 5.1, en el Control Panel o Panel de Control, seleccione "Add/Remove Programs".

En la ventana de "Add/Remove Programs", seleccione la opción "Add/Remove Windows Components" (Figura 5.2).

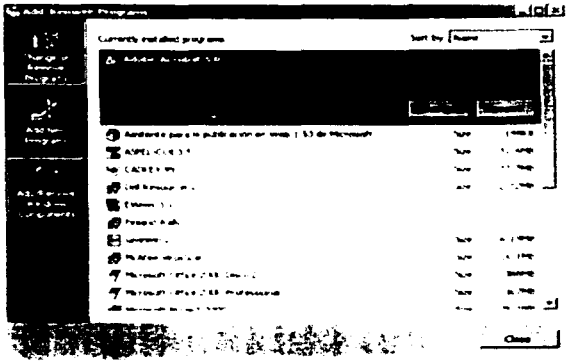


Figura 5.2
Agregando los servicios de Internet mediante el "Windows component Wizard"

En "Windows Component Wizard", seleccione "Internet Information Services" y hacemos click en "Details" (Figura 5.3).

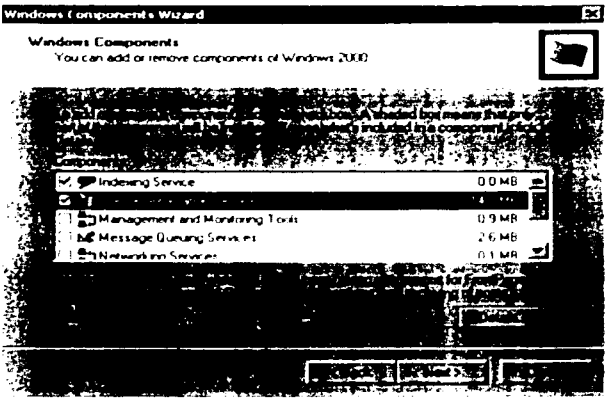


Figura 5.3
Habilitación de los servicios de Internet

En "Internet Information Services", seleccione las opciones requeridas por nuestro Sistema y haga click en el botón de "OK" (Figura 5.4)

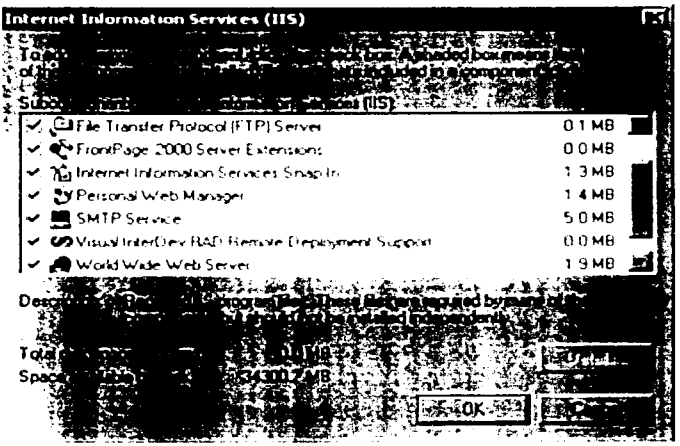


Figura 5.4
Selección de servicios de Internet según se requieran

En la pantalla de "Windows Component Wizard" (Figura 5.3), haga clic en "Next" y finalice la instalación.

Con lo anterior, usted ha habilitado los servicios de Internet en su servidor.

- **Creación del sitio**

Una vez habilitados los servicios de Internet, se procede a la creación del sitio, para ello, vaya a "Control Panel" y seleccione "Administrative Tools" (Figura 5.5).

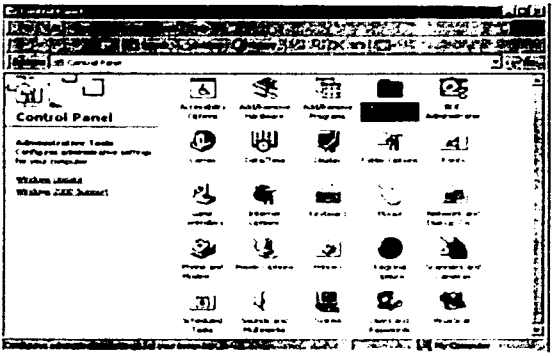


Figura 5.5

Selección desde el Panel de control de las herramientas administrativas para la creación del Sitio

En "Administrative Tools", seleccione "Internet Service Manager" (Figura 5.6).

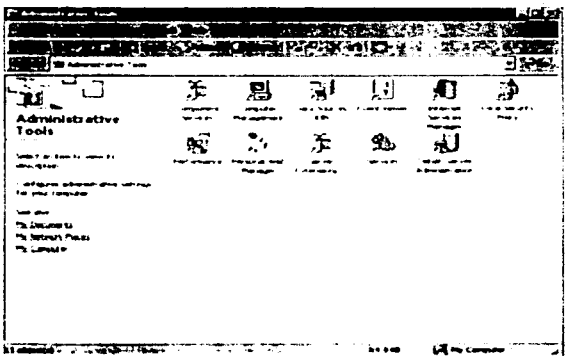


Figura 5.6

Seelección de Internet Service Manager para la creación del Sitio

En "Default Web Site", se procederá a crear un nuevo Directorio Virtual (botón derecho- New- Virtual Directory) (Figura 5.7)

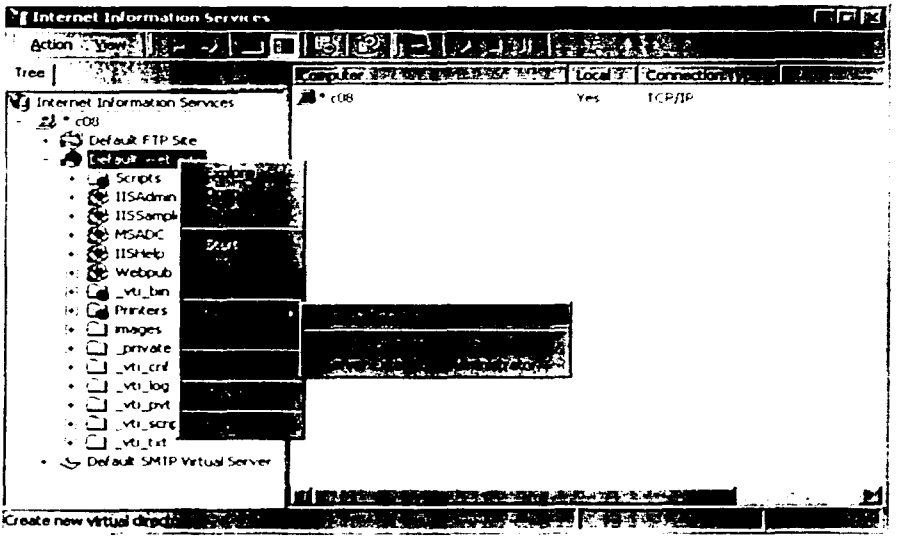


Figura 5.7
Creación del Directorio virtual en donde quedará alojado el Sitio

El alias propuesto para este nuevo directorio virtual es *Monitor*, el cual estará asociado al directorio físico del servidor, donde se copiará el código completo de la aplicación. El directorio físico propuesto es *Monitor*. El espacio requerido para albergar el código es aproximadamente 9 Megabytes.

Aparecerá un Wizard, que nos indicará que se está iniciando la creación de un Nuevo Directorio virtual (Figura 5.8)

Figura 5.8
Asistente (Wizard) para la creación del Sitio

En la ventana "Virtual Directory", proporcione el Alias del sitio, que en este caso llamaremos Monitor (Figura 5.9) y haga clic en "Next".

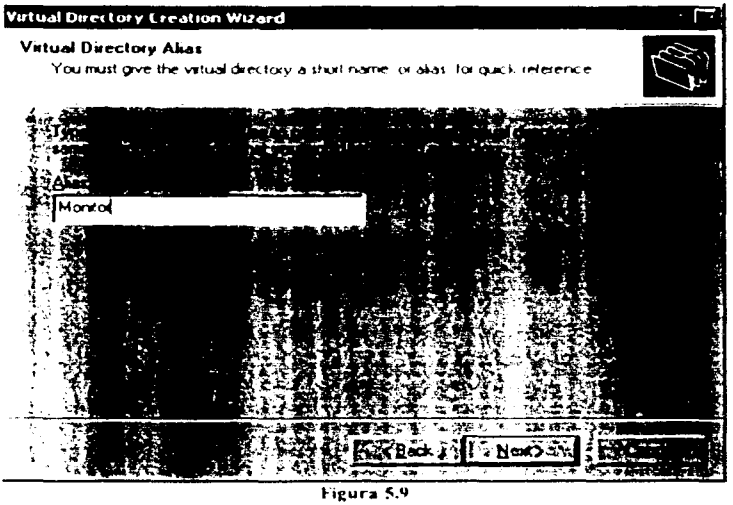


Figura 5.9
Denominacion del directorio virtual

En la ventana de "Web Site Content Directory", seleccione, mediante el botón "Browse", la ruta en la cual quedará alojado el sitio (Figuras 5.10 y 5.112).

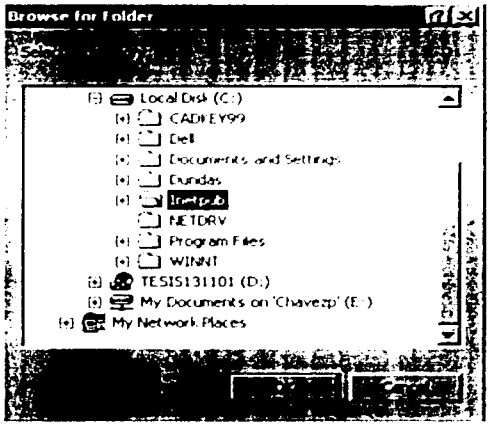


Figura 5.10

Selección del directorio de aplicaciones web en donde quedará alojado el Sitio

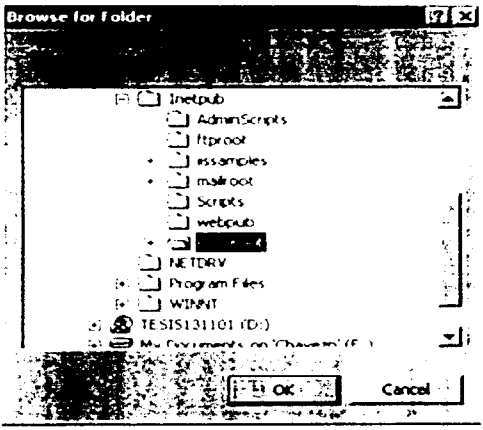


Figura 5.11

Selección del directorio raiz de la ruta en donde quedará alojado el Sitio

Asigne permisos sobre el Directorio virtual: *Permitir acceso de lectura* (Read) y *Permitir acceso a archivos de comandos (Run script (such as ASP))* como se muestra en la Figura 5.12.

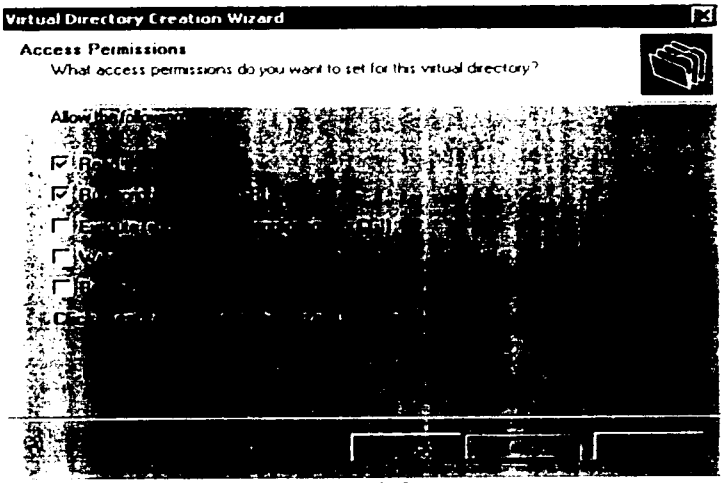


Figura 5.12
Asignación de permisos de acceso sobre el directorio virtual

Con lo anterior, se ha creado el Directorio Virtual satisfactoriamente.

Del Disco de Instalación del "Sistema de identificacion y control de acceso de personal en línea", ejecute el archivo de instalación del Software

- **La Base de Datos.**

Se requiere tener Instalado en el servidor SQL server 7.0 o superior.

Para ello, inserte en la Unidad de CD-ROM de su servidor el CD de instalación de SQL Server 7.0 o superior, se visualizará una pantalla de inicialización de SQL Server 7.0 (Figura 5.13)

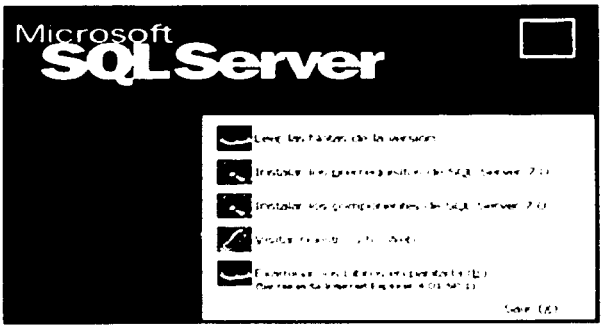


Figura 5.13
Pantalla de inicialización de la instalación de SQL Server 7.0

A continuación, haga clic en la opción "Instalar los componentes de SQL Server 7.0" (Figura 5.14)

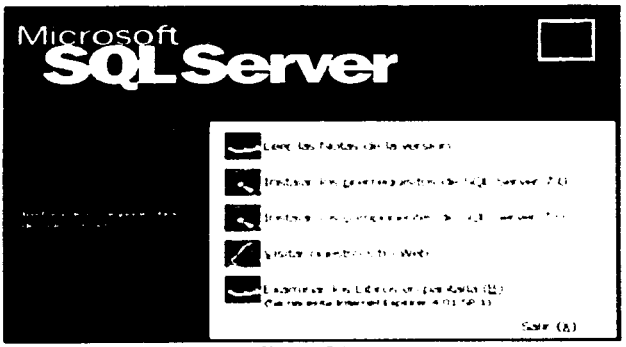


Figura 5.14
Selección de opción para instalación de componentes de SQL Server 7.0

A continuación, seleccione la opción "Instalación local: instalar en el equipo local" y haga click en el botón "Siguiente" (Figura 15)

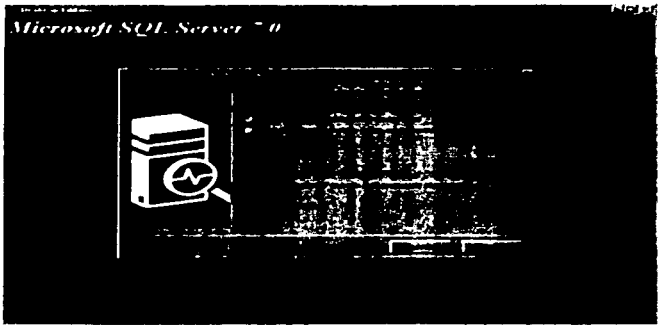


Figura 5.15
Instalación local del servidor de base de datos con SQL Server 7.0

A continuación, seleccione la opción "Típica" y haga click en el botón "Siguiente", con ello se inicializará la instalación de SQL Server 7.0. (Figura 5.16)

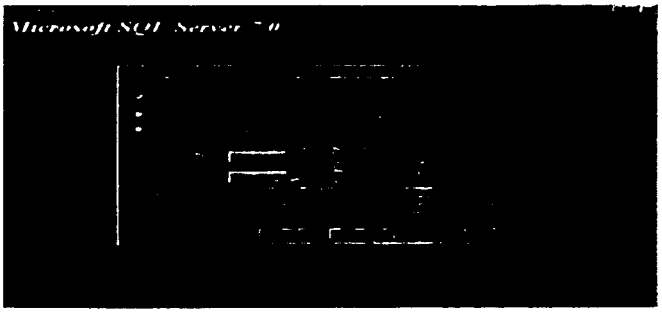


Figura 5.16
Selección de la instalaciónTípica de SQL Server 7.0

Para crear la Base de Datos con nombre ***dbMonitor*** y las tablas correspondientes, ejecute el script de la base de datos *dbMonitor.sql* desde *SQL Server 7.0* ó superior, que se encuentra en la carpeta /Monitor/SQL, dentro del CD de instalación.

Para ejecutar el script *dbMonitor.sql*, seleccione del Menú Tools (Herramientas) la opción Query Analizer (Figura 5.17)

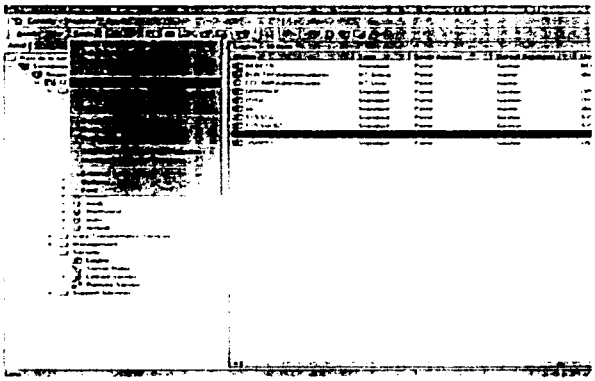


Figura 5.17
Inicialización del SQL Server Query Analizer

Dentro del Query Analizer, abra el archivo dbmonitor.sql y ejecute las sentencias dando clic en el ícono ó bien pulsando la tecla F5.

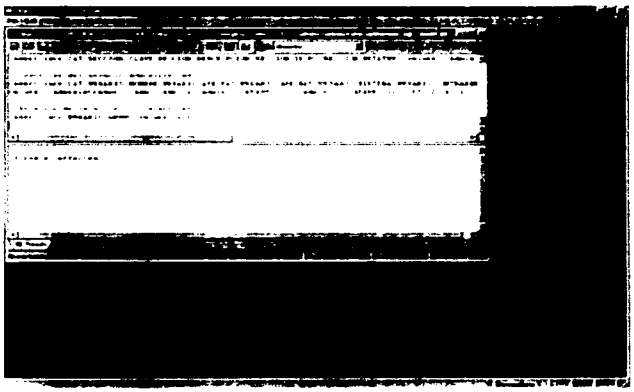


Figura 5.18
Ejecución de sentencias SQL desde el SQL Server Query Analizer

Con lo anterior, verifique que efectivamente existe una Base de Datos llamada dbmonitor en el Enterprise Manager (Administrador corporativo) de SQL Server 7.0, expandiendo la carpeta "Databases", en donde efectivamente existe una Base de Datos llamada dbmonitor, con ciertas propiedades que aparecen del lado derecho de la pantalla (Figura 5.19)

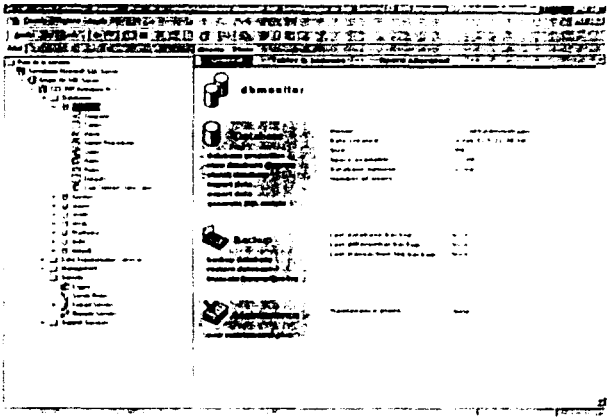


Figura 5.19
Propiedades de la base de datos dbmonitor

Para la Base de Datos dbmonitor, defina tamaños de los archivos de datos y de transacciones, establezca tamaños de 1MB de inicio, dando la posibilidad de crecer indefinidamente (Figuras 20 y 21)

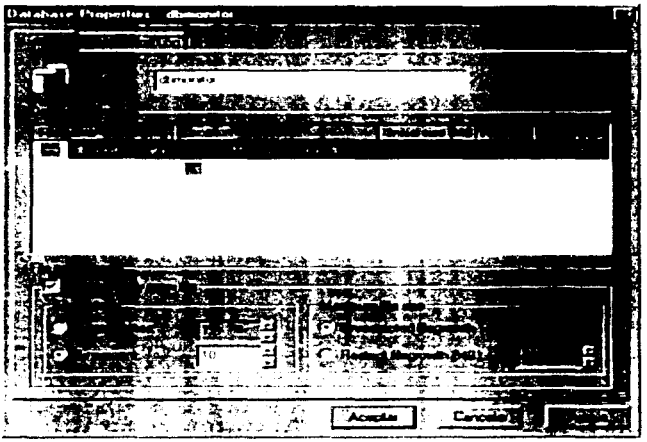


Figura 5.20

Definición del tamaño de la base de datos

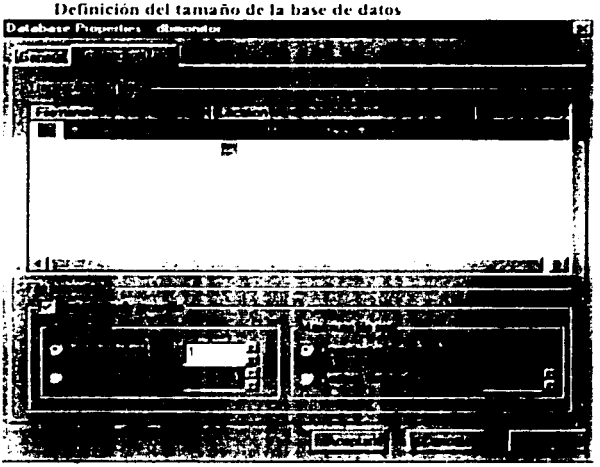


Figura 5.21
Definición del tamaño del archivo de transacciones log

Verifique que existan las tablas para la base de datos dbmonitor, posicionando el mouse en la base de datos dbmonitor y luego seleccione Tables (Tablas) (Figura 5.22)

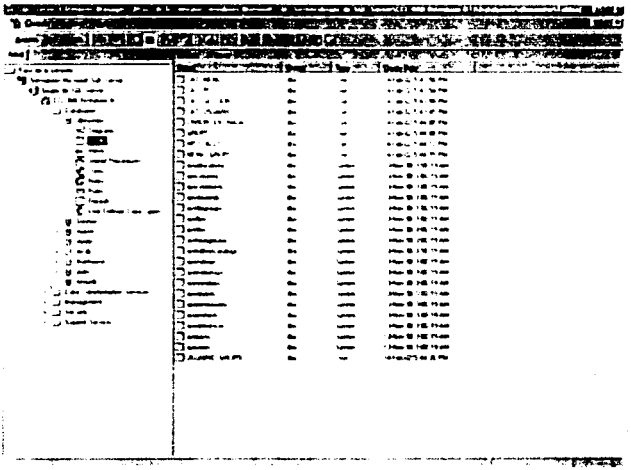


Figura 5.22

Verificación de la existencia de las tablas en la base de datos dbmonitor

A continuación, cree el usuario usr_monitor, expandiendo la carpeta "Security" (Seguridad) que se encuentra en la parte inferior del lado izquierdo de la pantalla, dentro del Enterprise Manager(Administrador corporativo) de SQL Server 7.0, y en "Logins" (inicios de sesión), con el botón derecho del mouse, seleccione New Login (Nuevo inicio de sesión), como se muestra en la Figura 5.23.

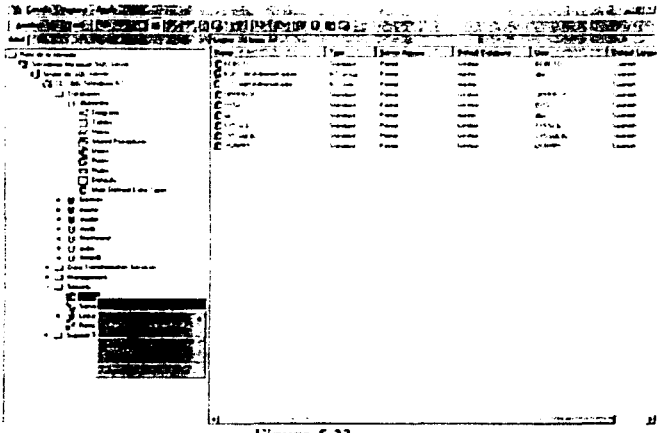


Figura 5.23
Creación de inicios de sesión con la opción "New Login"

- Seleccione la opción Security(Seguridad) y en Logins (Inicios de sesión), posicione el mouse sobre usr_monitor y con el botón derecho del mouse, seleccione la opción Properties (Propiedades) y haga click sobre esta última.
- En la pestaña "General", seleccione autenticación mediante SQL Server (SQL Server Authentication) y proporcione la contraseña (Password) con la cual el usuario usr_monitor accederá a la Base de Datos dbmonitor.
- En los valores predeterminados, seleccione la Base de Datos dbmonitor (Database) y el idioma (Language) Spanish (Figura 5.24)

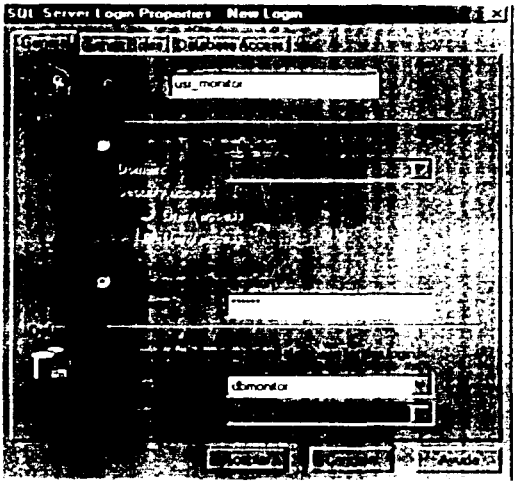


Figura 5.24
Definición del idioma español (Spanish) para la base de datos dbmonitor

En la pestaña "Server Roles" (Funciones del servidor) deje los valores que SQL Server 7.0 establece por omisión (Figura 5.25)

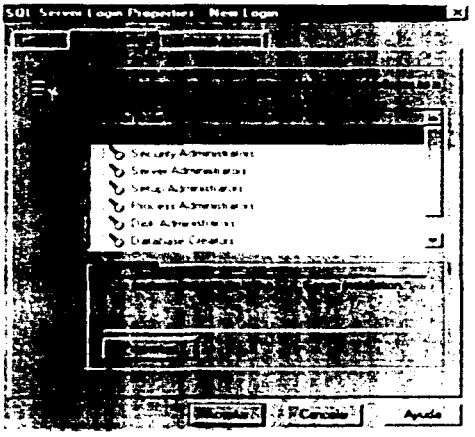


Figura 5.25
Asignación de roles predeterminados por SQL Server

En la pestaña "Database Access" (Acceso a base de datos) asigne privilegios al usuario usr_monitor; de acceso al público (public) dueño de la Base de Datos (db_owner), (Figura 26)

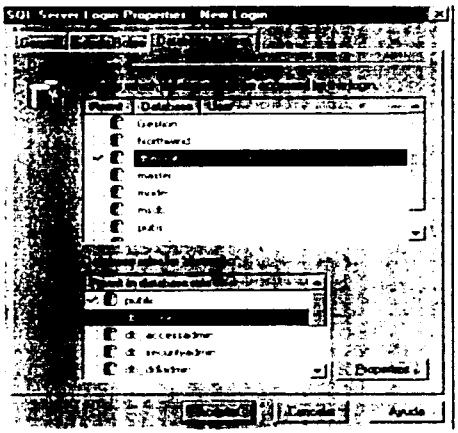


Figura 5.26
Asignación de privilegios de usuario a usr_monitor

Pulse el botón de aceptar y confirme su contraseña para acceder a la base de datos dbmonitor (Figura 5.27)

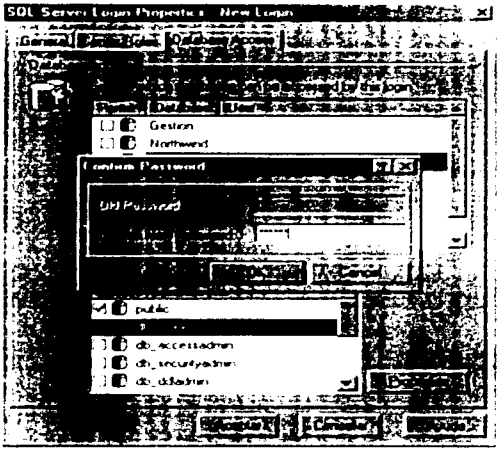


Figura 5.27
Confirmación de la contraseña asignada al usuario usr_monitor

Enseguida ejecute el script *IniciarMonitor.sql*, el cual inicializa las tablas principales del sistema para poder trabajar por primera vez. Este último script genera un usuario administrador con clave ***admin*** y contraseña ***admin***. (Figura 5.28)

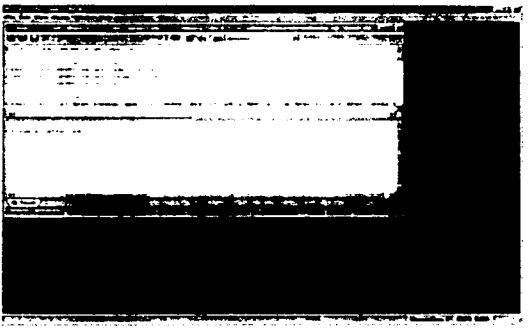


Figura 5.28
Ejecución del script IniciarMonitor.sql desde el SQL Server Analizer

Para establecer la conexión entre el sitio Web y la base de datos, se deberá configurar el archivo \Monitor\DLL\MONITOR.INI, en donde se especifica el nombre de la Base de Datos, el servidor donde reside la Base de Datos, así como el usuario y clave del usuario que tiene acceso a la Base de Datos (Figura 5.29)

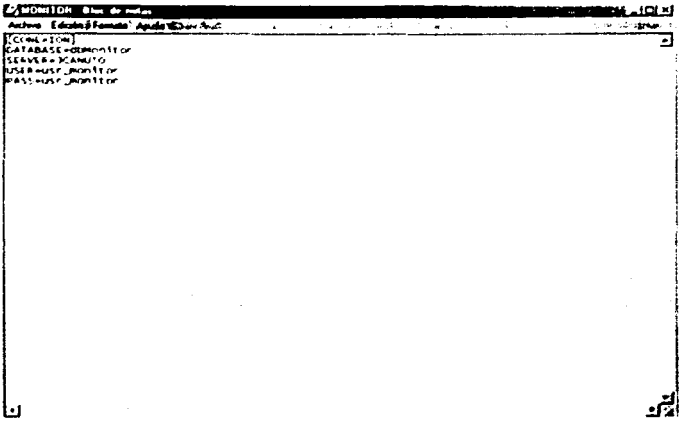


Figura 5.29
Archivo de inicialización de la base de datos

- **El correcto funcionamiento del sistema.**

Se deberá registrar en el servidor de Web el componente monitor.dll. Este componente es el corazón de la aplicación ya que es el que realiza las peticiones a la Base de Datos y nos devuelve la información en formato XML.

La forma de registrar el componente es la siguiente: En el botón de Inicio o Start de Windows presione y seleccione Run o Ejecutar y escriba la siguiente instrucción.

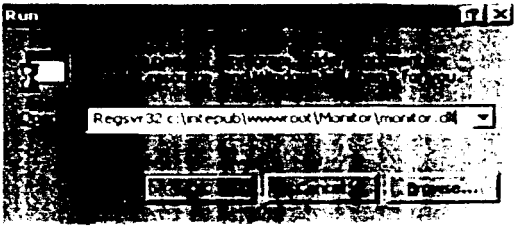


Figura 5.30
Registro en el servidor del componente monitor.dll

Se debe instalar el *Microsoft XML 4.0* que es el Parser encargado de soportar el lenguaje XML en el servidor.

Para ello, seleccione el archivo msxml4.exe y haga doble clic sobre él para iniciar la instalación de este software (Figura 5.14).

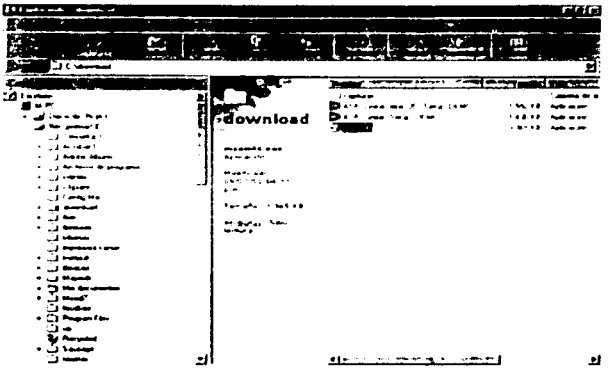


Figura 5.31
Instalación del Parser de XML

A continuación, aparecerá una pantalla de bienvenida al archivo de instalación del "Microsoft XML Parser y SDK"(Figura 5.32).

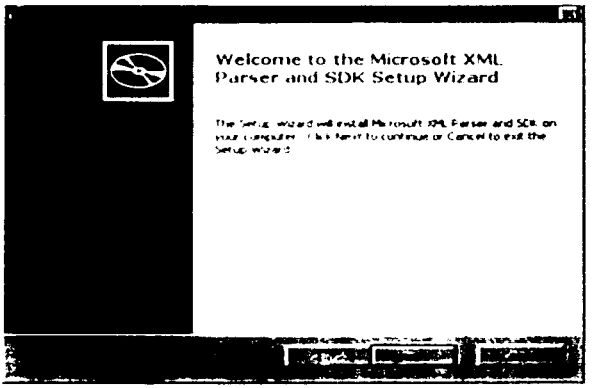


Figura 5.32
Pantalla de bienvenida a la instalación del Parser de XML

El archivo de instalación del "Microsoft XML Parser y SDK" le da la opción de efectuar una instalación completa (pulsando el boton de "Install Now") o personalizada (pulsando el botón "Customize"), se recomienda pulsar el boton "Install Now", con ello inicia la instalación del software en su servidor (Figura 5.33)

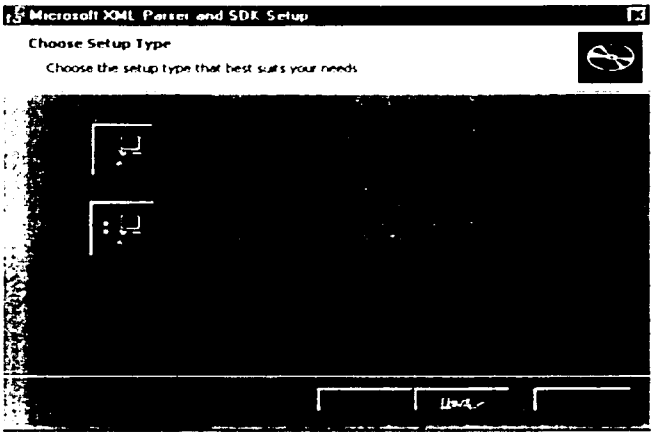


Figura 5.33
Pantalla con la cual continúa la instalación del Parser de XML

El archivo de instalación del "Microsoft XML Parser y SDK" lo guiará a través de la instalación del software y pulsando el botón de Next usted podrá continuar hasta el final de dicha instalación (Figura 5.34).

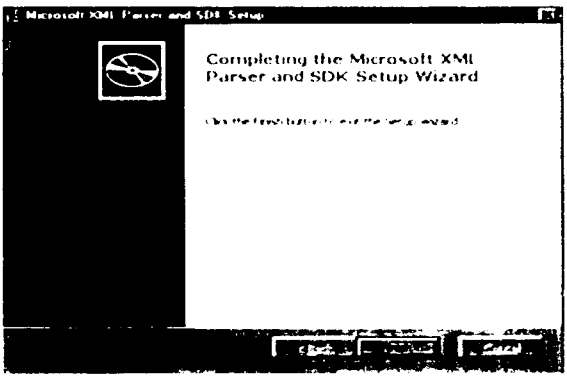


Figura 5.34
Pantalla que confirma la correcta instalación del Parser de XML

Para concluir la instalación del "Microsoft XML Parser y SDK", pulse el botón "Finish".

Se deberá instalar el componente generador de códigos de barra llamado, Asp_li1.exe versión demo que puede ser consultado y bajado en la dirección http://www.IDAutomation.com o bien buscarlo en la carpeta de utilerías en el CD de instalación. El archivo a ejecutar se llama Asp_li1.exe, haga doble clic sobre él para iniciar la instalación de este componente (Figura 5.35)

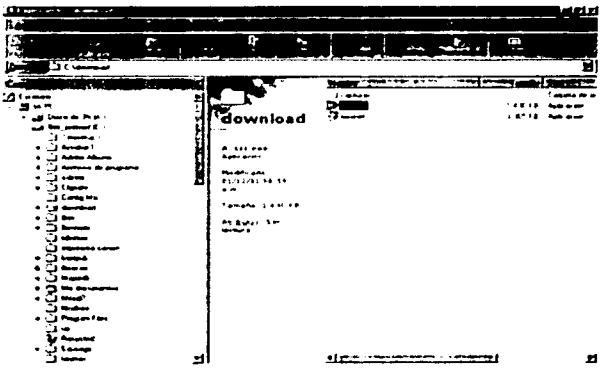


Figura 5.35
Archivo ejecutable para la instalación del componente generador de Códigos de barras

Posteriormente, le aparecerá en pantalla una ventana de inicio de instalación del Componente generador de Códigos de Barras (Figura 5.37)

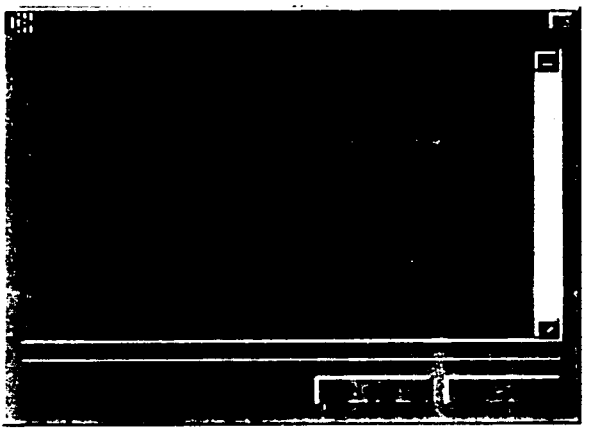


Figura 5.37
Pantalla inicial para la instalación del componente generador de Códigos de barras

Pulse el botón "Next" para continuar la instalación (Figura 5.37) y seleccione la ruta en la cual desea que quede instalado este componente, de acuerdo a la configuración de su servidor, luego pulse el botón "Start", con lo cual propiamente se instalará el componente (Figura 5.38)

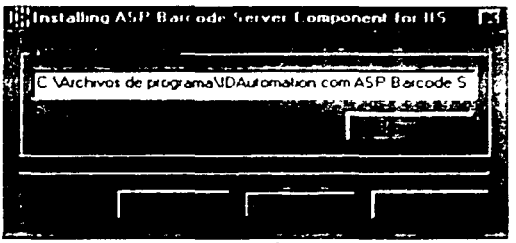


Figura 38
Selección de la ruta del servidor en la cual se instalará el componente generador de Códigos de barras

Finalmente, aparecerá una ventana en la cual se observa el avance de la instalación hasta llegar al 100%, momento en el cual, el componente quedará instalado en su servidor (Figura 5.39)

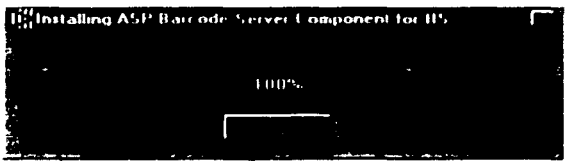


Figura 5.39
Aviso de que la instalación del componente generador de Códigos de barras se concluyó exitosamente

Finalmente, se instala en el servidor el software encargado de transferir archivos, en este caso imágenes. El software se llama *Dundas Upload*, y es un software libre que se puede obtener de la página www.dundas.com. Este software nos será de gran utilidad para subir archivos imagen al servidor y así poder ligarlas a los usuarios (Figuras 5.40 y 5.41)

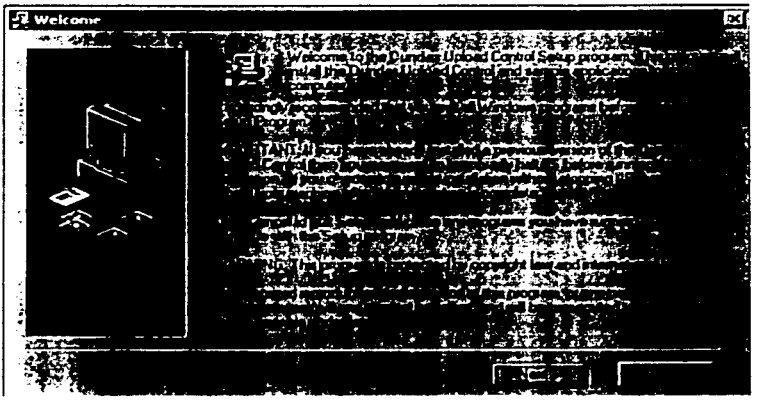


Figura 5.40
Pantalla de bienvenida a la instalación del componente Dundas para carga de archivos al servidor

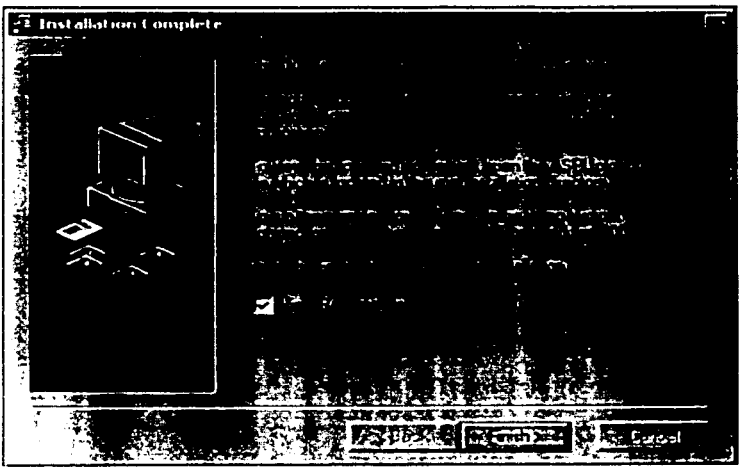


Figura 5.42
Pantalla que indica que el componente Dundas se ha instalado exitosamente en el servidor

Al final de este manual, se encuentra un anexo que contiene la relaciones de archivos que se ejecutan para cada página del sistema.

Manual de Usuario del Sistema de Identificación y Control de Acceso de Personal en Línea

Introducción

El presente manual está dirigido a todos los usuarios del *Sistema de identificación y control de acceso de personal en línea* , a los Administradores del Sistema, así como al personal encargado del control de acceso de empleados a las instalaciones de un Centro de trabajo (vigilancia).

Convenciones

En el *Sistema de identificación y control de acceso de personal en línea*, existen varias tareas relacionadas con los catálogos, a continuación se mencionan las más comunes y la forma de ejecutarlas.

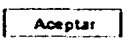
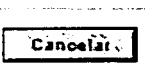
Tareas	Forma de llamar la tarea	Botón	Nombre
Agrega un nuevo registro	Haciendo click con el botón izquierdo del ratón sobre el botón.		Botón para Agregar un nuevo registro.
Cambiar el estado del registro	Haciendo click con el botón izquierdo del ratón sobre el botón.		Botón para Eliminar un registro.
Editar un registro	Haciendo click con el botón izquierdo del ratón en el primer campo de la página.		
Grabar el registro	Haciendo click con el botón izquierdo del ratón en el botón "Aceptar".		Botón "Aceptar"
Cancelar cambios	Haciendo click con el botón izquierdo del ratón en el botón Cancelar.		Botón "Cancelar"

Tabla 5.1.1
Tareas relacionadas con los Catálogos para el presente Sistema

El sistema

El *Sistema de identificación y control de acceso de personal en línea*: Es una aplicacion que corre bajo entorno web y que permite controlar el acceso del personal que labora en un Centro de trabajo, así como el monitoreo de su ubicación en un momento dado. Para ello, se requiere contar con una configuración en red para la autenticación del personal, en donde se cuenta con equipo de cómputo intercomunicado a través del protocolo TCP/IP, dentro de una Intranet, Extranet o Internet (Figura 5.1.2)

El presente Sistema es de los llamados distribuidos, los cuales deben contar con un servidor de base de datos, un servidor de aplicaciones y las computadoras cliente.

El *servidor de aplicaciones*: Se encarga de procesar todas las peticiones de los clientes, en función de la información contenida en la base de datos.

Para nuestro Sistema un solo servidor contendrá tanto a la base de datos como a las aplicaciones, mientras que los clientes serán Computadoras Personales conectadas al servidor de aplicaciones.

Las *peticiones de las computadoras cliente*: Se realizarán mediante un browser (Microsoft Internet Explorer, Netscape Navigator, etc.), por lo tanto no se requiere de la instalación de software adicional.

La Figura 5.1.2 muestra el diseño general del sistema dentro de una Intranet, aunque como se puede apreciar con la línea punteada, puede aplicarse a una red de cobertura mundial, como lo es Internet.

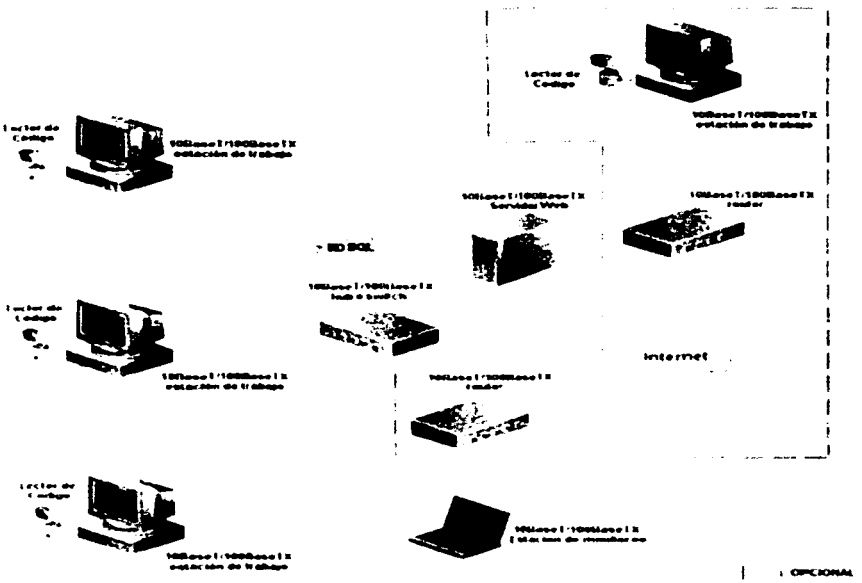


Figura 5.1.2
Esquema general para el Sistema dentro de una Intranet

Inicio de sesión

Para ingresar al sistema únicamente se debe colocar la dirección electrónica del sitio en el navegador http://NombreDelServidor/monitor para obtener la página de inicio que se muestra en la Figura 5.1.3.

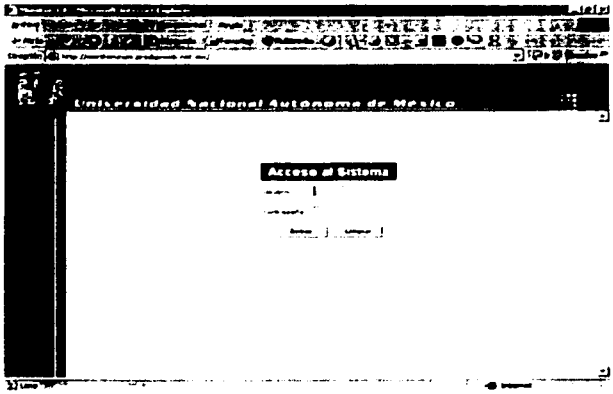


Figura 5.1.3
Pantalla de acceso al Sistema

En la página principal (Figura 5.1.3) se solicita el nombre de usuario y el código de autorización, los cuales serán validados contra la información contenida en la base de datos para proporcionar o negar el acceso al sistema. Cuando la información proporcionada no está contenida en la base de datos el sistema muestra un mensaje de error (Figura 5.1.4), por el contrario si la información proporcionada es correcta, se hacen visibles o invisibles las opciones del menú en función de las jerarquías de usuario.

Figura 5.1.4
Mensaje de error generado al haber proporcionado una clave de usuario o contraseña no válidas

En la Figura 5.1.5 se muestra el diagrama de navegación general del sistema:

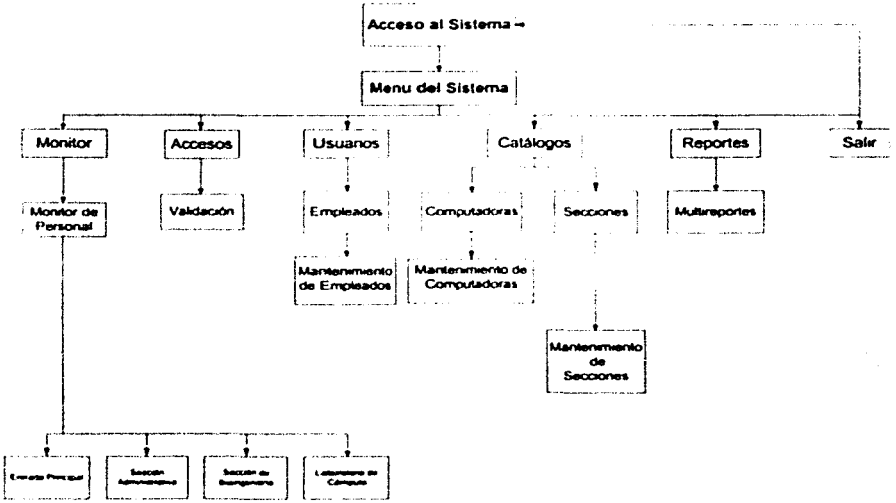


Figura 5.1.5
Diagrama general de navegación para el Sistema

Para la descripción del menú debemos de considerar lo siguiente:

El sistema puede registrar el acceso a una o varias secciones de un inmueble a través de computadoras que deberán estar asociadas a cada sección, en una relación de uno a uno; es decir cada sección deberá tener asociada una sola computadora que controlará el acceso a las instalaciones como lo muestra la Figura 5.1.2.

Las secciones son necesarias para el registro de usuarios, debido a que el sistema requiere que los usuarios estén asociados a una o más secciones.

Por lo tanto, seguiremos esta secuencia para la descripción del menú:

- Catálogo Computadoras
- Catálogo secciones
- Empleados
- Accesos
- Monitor
- Visitas
- Alertas
- Reportes

En la Figura 5.1.6 se muestra el menú con todas las posibles opciones:

Figura 5.1.6
Menú de opciones para el Sistema

El menú Catálogos tiene las opciones de "Computadoras" y "Secciones"(Figura 5.1.7)

Figura 5.1.7
Menú Catálogos

Catálogo Computadoras

Al seleccionar la opción del menú Catálogo->Computadoras (Figura 5.1.8), mostrará los datos generales de las computadoras que integran el sistema: la descripción, el estado y la dirección IP asociada.

En esta página sólo es posible cambiar el estado de las computadoras de "Activo" a "Inactivo" o viceversa, mediante el botón "Eliminar", el Sistema siempre presenta un mensaje de confirmación en cada cambio. Al editar o agregar un nuevo registro aparece la página mostrada en la Figura 5.1.9.

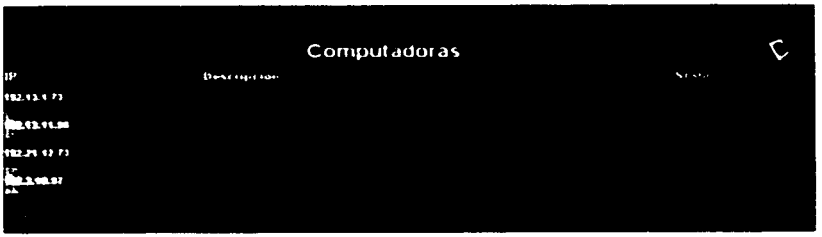


Figura 5.1.8
Catálogo de Computadoras

Cada computadora registrada en el sistema debe contener la siguiente información: Una dirección IP única, una breve descripción de la computadora, su estado (Activo, Inactivo), la fecha de cambio de estado y la fecha de baja que el sistema asigna de forma automatica al realizar los cambios de estado.

Para las direcciones IP es necesario consultar al administrador de la red para que otorgue las adecuadas.

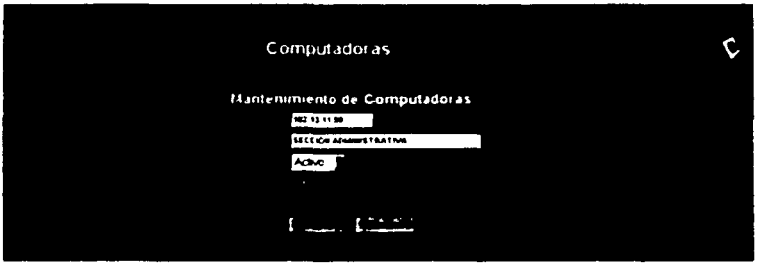


Figura 5.1.9
Pantalla para el mantenimiento del Catálogo de Computadoras

Secciones

La opción del menú Catálogo-Secciones presenta la página mostrada en la Figura 5.1.10, con los datos generales para cada sección.

Cada renglón representa una sección, en esta página sólo es posible cambiar el estado de la sección mediante el botón eliminar, el sistema para cualquier cambio de estado siempre presenta un mensaje de confirmación.

La edición del registro se realiza mediante el campo Clave y el sistema muestra la página de la Figura 5.1.11.

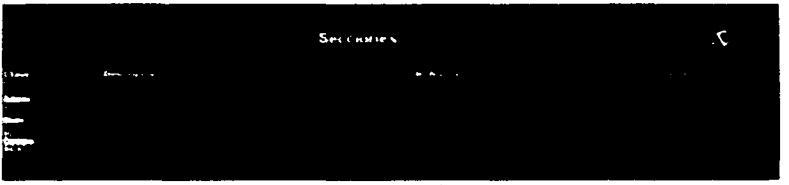


Figura 5.1.10
Catálogo de Secciones

La información que incluye cada sección es la siguiente

La clave de la sección la cual debe ser única, una breve descripción de la sección, la dirección IP asociada para poder ligar la computadora a un punto de acceso a las instalaciones, el estado de la sección que puede ser "Activo" o "Inactivo", la fecha de

cambio de estado y la fecha en que se da de baja a la sección, estas dos últimas son actualizadas por el sistema en forma automática.

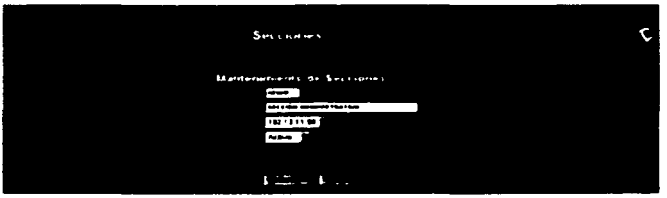


Figura 5.1.11
Pantalla para mantenimiento al Catálogo de Secciones

Al seleccionar la opción del menú usuarios (Figura 5.1.12) se muestran los datos generales de los usuarios del sistema.

En esta página sólo es posible cambiar el estado del usuario de "Activo" a "Inactivo" o viceversa, el Sistema siempre mostrará un mensaje de confirmación en cada cambio de estado.

La edición del registro se realiza mediante el campo CB(Código de Barras) y al ser seleccionado se muestran todos los datos del usuario (Figura 5.1.13)

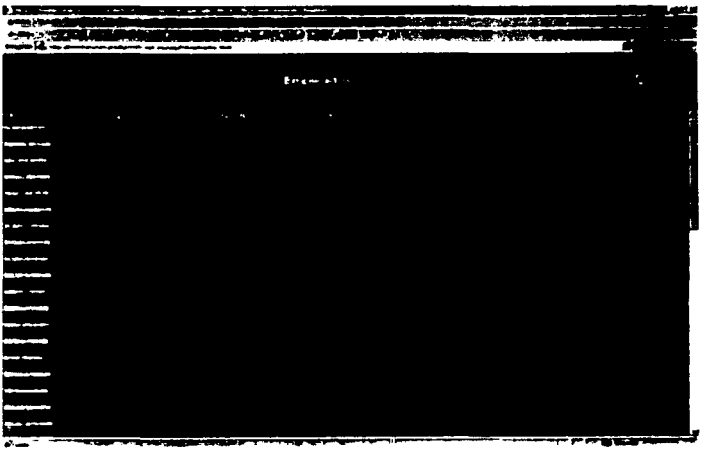


Figura 5.1.12
Catálogo de Empleados

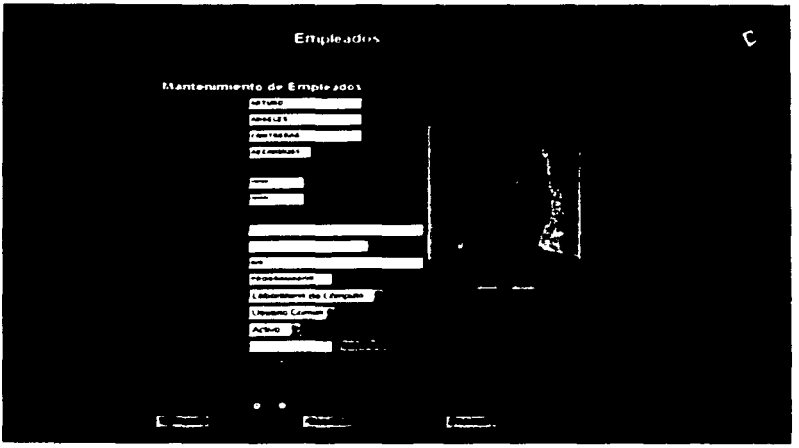


Figura 5.1.13
Pantalla para mantenimiento a Catálogo de Empleados

La tabla siguiente contiene los datos que el sistema solicita para cada usuario registrado, la primera columna contiene el nombre del campo, la segunda columna contiene la descripción del campo y la tercera indica si el campo requiere forzosamente valores.

Nombre del campo	Descripción	Requiere valor
Nombre	Nombre del usuario	Si
Apellido Paterno	Apellido paterno del usuario	Si
Apellido Materno	Apellido Materno del usuario	Si
RFC	Registro Federal de Contribuyentes	Si
Clave	Clave de acceso al sistema	Si
Contraseña	Contraseña de acceso al sistema	Si
Confirma contraseña	Contraseña de acceso al sistema, debe ser igual a la proporcionada en el campo contraseña	Si
CB Usuario	Código de barras del usuario, compuesto por el RFC y un número consecutivo proporcionado de manera automática por el Sistema	Si
E-Mail	Dirección electrónica del usuario	No
Teléfono	Teléfono del usuario	No
Dirección	Dirección del usuario	No
Cargo	Cargo del usuario dentro de la organización	No
Sección	Sección a la cuál el usuario pertenece	No
Jerarquía	Jerarquía que ocupa dentro del sistema (tipo de usuario)	No
Status	Estado que tiene en el sistema (activo, inactivo)	No

Foto	Ruta de acceso al archivo gráfico que contiene la fotografía digitalizada del usuario	Si
Fecha Alta	Fecha de registro del usuario, de manera automática el sistema proporciona el valor	No
Fecha Cambio	Fecha de cambio de estado de usuario, en forma automática el sistema proporciona el valor	No
Fecha Baja	Fecha de baja del usuario, de manera automática el sistema proporciona el valor	No
Acceso al sistema	Indicador de acceso al sistema	No

Las consideraciones que se deben de tener para el registro de usuarios son las siguientes:

- Existen tres jerarquías o tipos de usuarios: El Administrador, el Monitor, el Usuario/el Visitante.
- En base a las jerarquías de los usuarios se otorgan los permisos para el menú, quedando de la siguiente forma: El Administrador tendrá derecho a todas las opciones, el Monitor tendrá activada solamente la opción de accesos, al Usuario sólo se le activará la opción de multireportes y el Visitante se comportará de manera similar al Usuario, sólo que en el momento de generarle su credencial, esta no tendrá fotografía y en lugar de ello, mostrará la leyenda "Visitante".

Para agregar la fotografía del usuario existen dos formas: la primera consiste en proporcionar la ruta directamente en la caja de texto y la segunda es seleccionando el botón [Examinar...], el cuál activa la ventana de diálogo predeterminada de Windows, en esta ventana es posible navegar entre los diferentes directorios a los cuales se tiene acceso, tanto en forma local como a los que pertenezcan a la red (Figura 5.1.14), para seleccionar el archivo sólo se necesita ubicarse en el nombre deseado y oprimir el botón "Abrir".

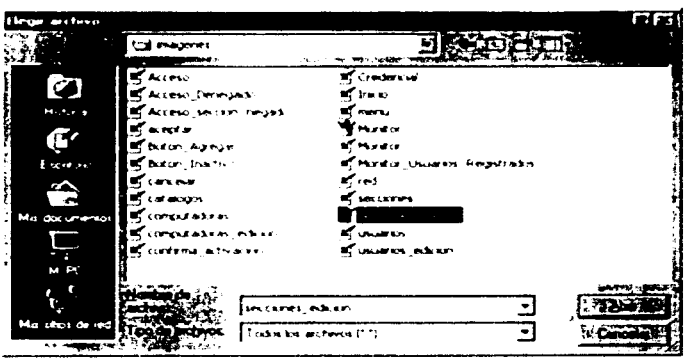


Figura 5.1.14

Selección de imagen a subir al servidor para asignación de fotografía para credencial del Empleado
La resolución del archivo se recomienda sea de 200 X 250 pixeles con un tamaño no mayor a 50KB.

El botón Credencial muestra la página de la Figura 5.1.15, la cual es una vista previa de la impresión de credenciales y contiene los siguientes datos que identifican al usuario: Nombre, Apellido paterno, Apellido materno, Cargo, Sección a la cual tiene permiso de ingreso y el Código de Barras.

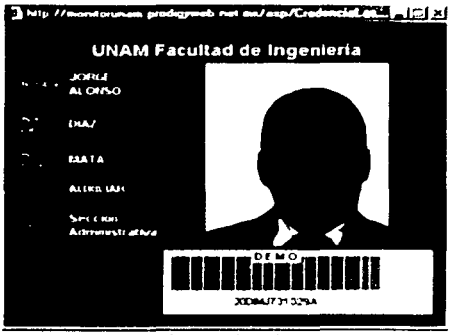


Figura 5.1.15
Vista previa de la credencial del empleado

Accesos

En un inmueble generalmente se cuenta con una entrada principal y dentro de él diferentes secciones, en donde es necesario registrar el acceso. El Sistema es capaz de realizar el registro de las diferentes entradas como lo muestra la Figura 5.1.16. En la figura se puede observar que para poder ingresar a cualquier sección es necesario haber ingresado por la entrada principal, y de forma inversa para poder salir por la entrada principal es necesario no encontrarse dentro de ninguna sección.

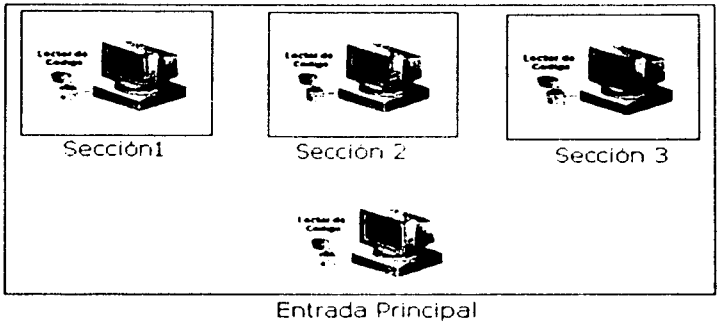


Figura 5.1.16
Esquema que muestra las diferentes entradas del Centro de trabajo con sus respectivos lectores de Código de barras

La opción del menú accesos muestra la página de la Figura 5.1.17; cada punto de control debe de tener esta página visible cada vez que un usuario desee ingresar a la sección.

Todos los usuarios podrán ingresar a todas las secciones, pero en caso de que no se tenga la autorización correspondiente, el Sistema generará una alerta en el monitoreo (ver sección de monitoreo). Cuando se ingrese un Código de Barras no registrado, el sistema generará un mensaje de error y solicitará nuevamente el ingreso del Código de Barras (Figura 5.1.18)

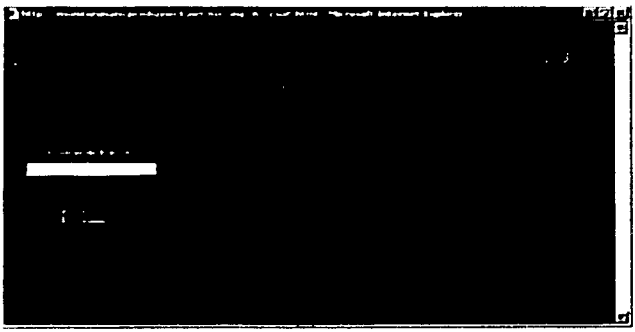


Figura 5.1.17
Página para la toma del Código de barras de la credencial del Empleado

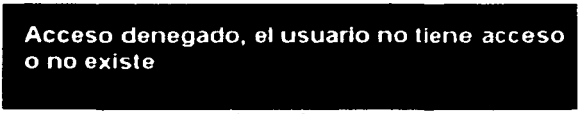


Figura 5.1.18
Pantalla que muestra un mensaje de error al intentar acceder a una sección con un Código de barras no existente en la base de datos del Sistema

Cuando el Código de Barras pertenece a un usuario con permisos de ingresar a la sección el Sistema muestra el mensaje de bienvenida de la Figura 5.1.19

Figura 5.1.19
Pantalla que muestra datos del usuario que ha ingresado por la Entrada principal

Consideremos 2 situaciones que se pueden presentar en el ingreso y salida de personal por la entrada principal:

- Se presenta cuando un usuario desea ingresar a una sección sin haber registrado la entrada en la principal, en este caso el Sistema muestra el mensaje de la Figura 5.1.20

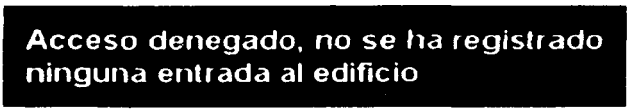


Figura 5.1.20
Mensaje de error generado cuando un usuario intenta ingresar a una sección sin haber antes ingresado por la Entrada principal

- Cuando un usuario ha ingresado por la entrada principal y está dentro de una sección, pero desea salir por la entrada principal, el Sistema muestra el mensaje de la Figura 5.1.21.

Figura 5.1.21
Mensaje de error generado cuando un Empleado intenta ingresar a otra sección sin haber antes abandonado la sección en la cual estaba

Monitoreo

El monitoreo del personal que ha ingresado a las instalaciones se lleva a cabo por secciones, como se muestra en la figura 5.1.22. Cada sección se representa por un rectángulo que contiene tanto el nombre de la sección como la cantidad de usuarios con entrada registrada en el Sistema en ese momento, las alertas se representan mediante puntos rojos en la parte derecha de la sección. Los usuarios se representan mediante diferentes iconos, de acuerdo a su jerarquía.

Cada usuario estará representado por un icono, dependiendo del grupo al que pertenezca. (Figura 5.1.22)

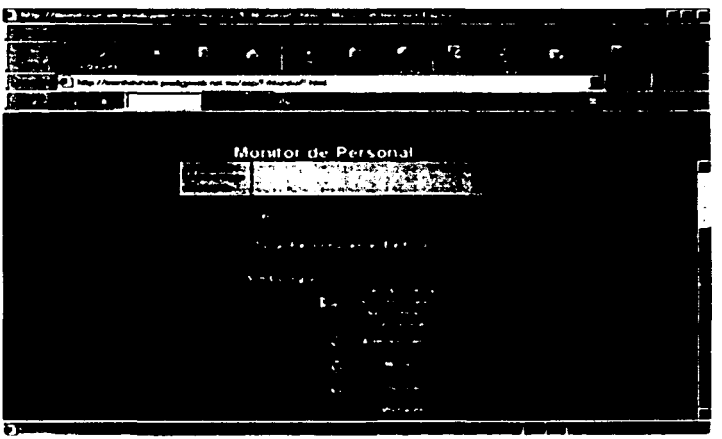


Figura 5.1.22
Simbología para la representación de usuarios que se encuentran en alguna sección del Centro de trabajo

Cada una de las secciones del Edificio se representan por un rectángulo.

La entrada principal se muestra en la Figura 5.1.23, y en el momento actual tiene registrados 10 usuarios.

Figura 5.1.23
Usuarios que se encuentran en la Entrada principal

La sección de Bio-Ingeniería se muestra en la Figura 5.1.24 y actualmente no presenta ninguna persona en su interior (Figura 5.1.25)

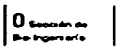


Figura 5.1.24
Representación visual de la sección de Bio-Ingeniería

Cuando alguna de las secciones tiene registradas entradas de usuario cambia el color en la que es mostrada, la Figura 5.1.25 muestra la sección Administrativa con 10 usuarios registrados.

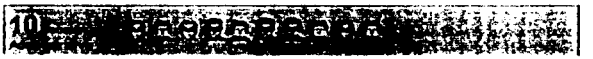
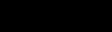


Figura 5.1.25
Usuarios que se encuentran en la sección Administrativa

El monitoreo además, puede realizarse a nivel sección, al hacer click sobre el ícono que representa a los usuarios, con lo cual, el sistema muestra la página de la Figura 5.1.26, donde se aprecian los datos pertenecientes al usuario del cuál se registro la entrada.

Figura 5.1.26
Datos del empleado generados al hacer doble click con el ratón sobre uno de los empleados dentro de una sección determinada del Centro de trabajo

Visitas

Las visitas al inmueble quedan registradas a través de la opción del menú Accesos, mediante el botón  .

La opción Visitas se selecciona al hacer click sobre el botón visitas, la página muestra a los visitantes registrados en el sistema, teniendo la opción de agregar nuevos visitantes o bien realizar cambios a los existentes, mediante el campo CB (Código de barras), la Figura 5.1.27 muestra el registro de visitantes.

Figura 5.1.27
Visitantes registrados en el Sistema

Los datos que contiene el registro de los visitantes se pueden apreciar en la Figura 5.1.28

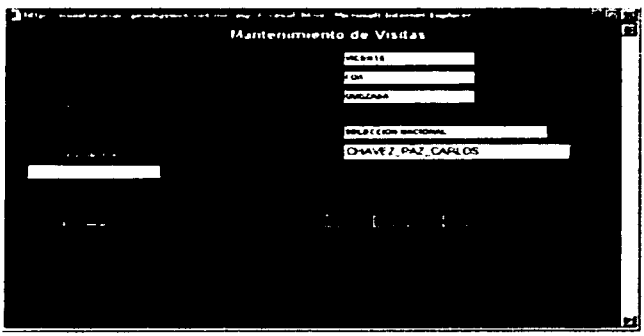


Figura 5.1.28
Pantalla para mantenimiento a visitantes

Al igual que en menú usuarios podemos realizar una impresión de la credencial del visitante a través del botón credencial Credencial.

La página mostrada cuando ingresa un visitante es muy similar a la mostrada cuando ingresa un usuario, la figura 5.1.29 muestra el ingreso de un visitante.

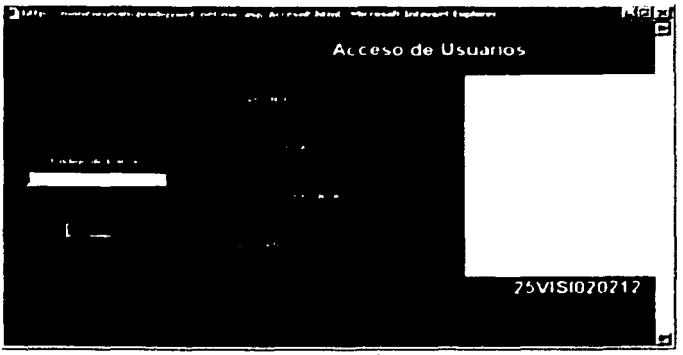


Figura 5.1.29
Acceso de visitantes

Cuando el sistema niega el acceso al visitante las páginas mostradas son iguales a las de los usuarios(ver sección accesos).

Salida de las instalaciones

Cuando una persona abandona las instalaciones, el Sistema muestra el mensaje de la Figura 5.1.30.

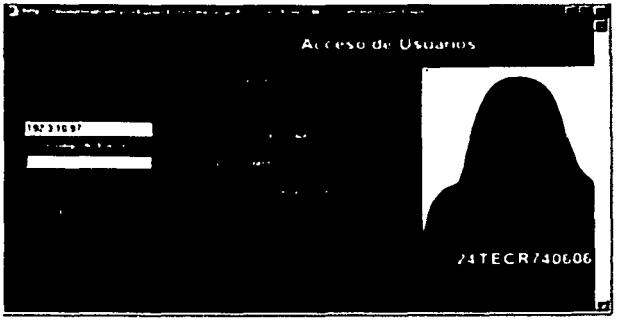


Figura 5.1.30

Salida de las instalaciones

Alertas

Las alertas se muestran en la página de monitoreo, mediante señalizaciones en la sección, la Figura 5.1.31 muestra dos alertas, una registrada en la Sección de Bio-Ingeniería y otra en la Sección Administrativa.

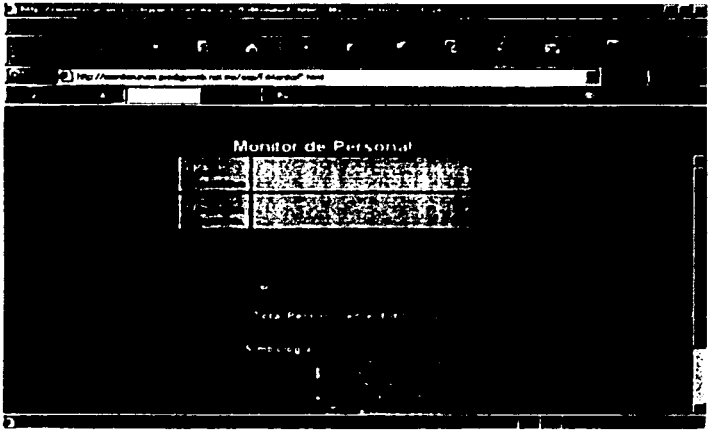


Figura 5.1.31
Pantalla que muestra las alertas en los accesos, representadas por puntos rojos

Haciendo click con el botón izquierdo del ratón, sobre la alerta (botón rojo), podemos ver sus datos (Figuras 5.1.32).

Figura 5.1.32
La representación de alertas mediante puntos rojos

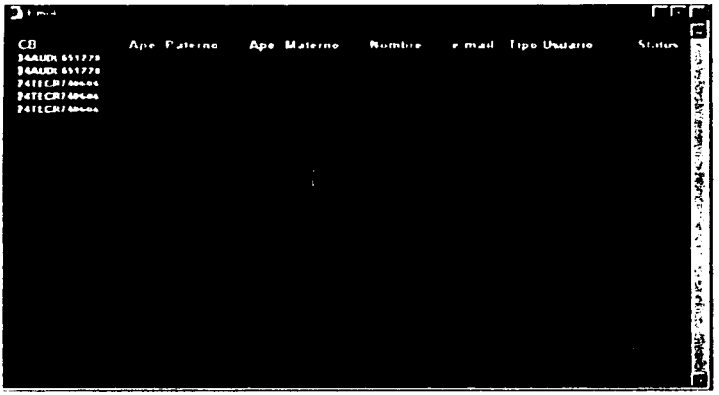


Figura 5.1.33
Histórico de accesos con alertas

Para cada alerta pueden existir uno o más registros que la generaron, la Figura 5.1.33 muestra una alerta para la sección administrativa. Para que dejen de visualizarse las alertas, es necesario hacer clic con el botón izquierdo del ratón sobre el botón.

Visitas

Para ver la información de las Visitas o visitantes, se requiere seleccionar la opción Accesos del Menú, y hacer clic con el botón izquierdo del ratón, en el botón con lo cual, en la parte derecha de la pantalla, se desplegarán los datos de las personas visitantes (Figura 5.1.34).

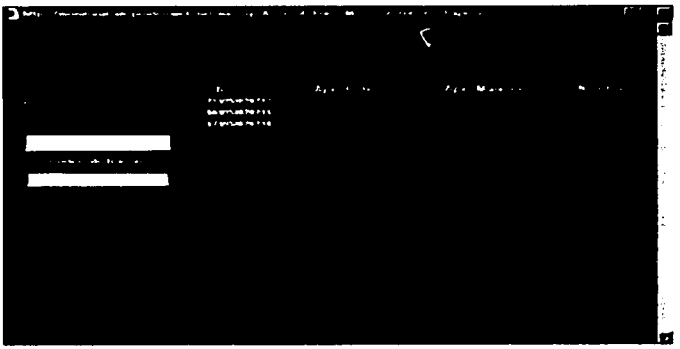


Figura 5.1.34

Pantalla de accesos de visitantes

Es posible dar mantenimiento a los datos de las Visitas, haciendo click en el campo CB (Código de Barras; Figura 5.1.34). En donde, una vez efectuado algún cambio a alguno de los Datos de la visita, debe pulsarse el botón "Aceptar", para confirmar los cambios. Finalmente, si lo que se desea es descartar los cambios, se requiere pulsar el botón "Cancelar".

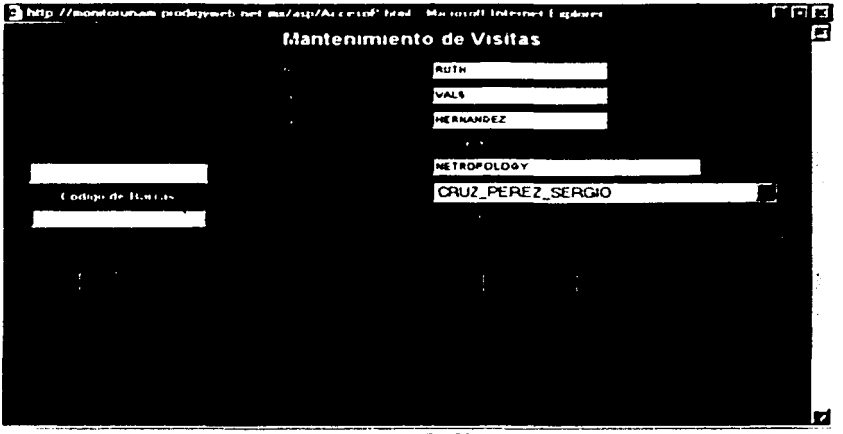


Figura 5.1.35
Pantalla para mantenimiento a visitas

Reportes

Al seleccionar la opción reportes se despliega el submenú de multireportes, el cual nos muestra la página de la Figura 5.1.36.

En esta opción del Sistema se obtiene la información histórica, que se encuentra almacenada en la base de datos de los registros de entradas y salidas por sección.

Los reportes pueden generarse de manera global, para todas las secciones y todos los usuarios, o bien, por cada sección, con todos los usuarios o para cada usuario en particular.

Las secciones y los usuarios existentes en el Sistema se muestran en listas desplegables, la Figura 5.1.37 muestra las listas de secciones y usuarios.

Estos reportes además pueden ser obtenidos por periodos de tiempo, en el caso de que se desee obtener toda la información contenida en el registro de entradas, se debe seleccionar.

de la lista desplegable "Usuario", "Todos" y en "Sección" también "Todos", sin proporcionar fechas, con lo cual, el Sistema muestra todos los accesos registrados desde su puesta en marcha.

Las fechas deben proporcionarse en las cajas disponibles que corresponden al dia, mes y año, al hacer click sobre alguna caja se muestran los valores que estas pueden tomar (Figura 5.1.37)

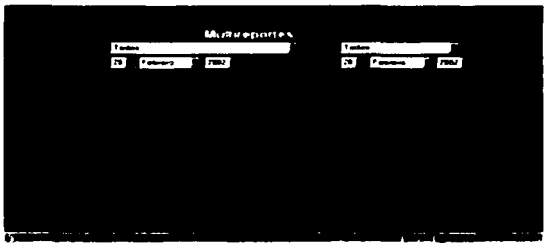


Figura 5.1.36
Pantalla para generación de reportes por múltiples parámetros

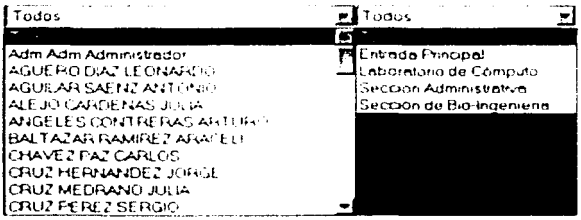


Figura 5.1.37
Parámetros y sus valores para la generación de reportes

En caso de ingresar una fecha no válida, el Sistema generará un mensaje de error (Figura 5.1.38).

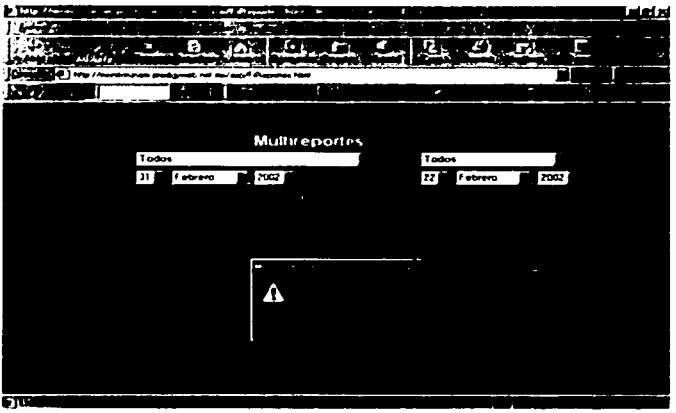


Figura 5.1.38
Validación de parámetros incorrectos

Cuando no existe información en el Sistema, se muestra el mensaje de error de la Figura 5.1.39.

ERROR
CODIGO Error Error
No existe información histórica

Figura 5.1.39
Generación de mensaje de error cuando no existe información histórica en la base de datos, para un reporte dado

La Figura 5.1.40 muestra un reporte de la entrada principal para un periodo del 01/01/2002 al 22/02/2002.

Figura 5.1.40
Pantalla que muestra datos de un reporte generado

Hay que recordar que existen diferentes tipos de Reportes como lo pueden ser:

- Globales, de todas las áreas y de todas la personas.
- Solo un área especifica.
- Monitoreo personal.
- Por fecha determinada

CONCLUSIONES

Conclusiones

Sin lugar a dudas, en los últimos años los Sistema de identificación han dejado de ser un tema secundario y se ha convertido en uno de los temas más importantes hoy en día en un centro de trabajo.

Existen distintos tipos de sistemas de identificación y control de acceso de personal, están aquellos que almacenan datos de quienes entraron, que día y a que hora y los que son autónomos y no guardan ningún tipo de información, pero si discriminan que individuo ingresa y cual no. Es decir la importancia fundamental esta en evitarle el ingreso a quien no lo tiene permitido, pero además registrar los accesos a cada nivel.

Las caracteristicas fundamentales del sistema desarrollado son:

- La interfaz es amigable y sencilla, que lejos de ser un software con gráficos complicados, se vuelve sencillo al tener una visualización de tipo Web.
- Monitoreo, las 24 horas del día, si existe o no personal autorizado en áreas claves de la empresa.
- Cuenta con la funcionalidad de operar tanto en una Intranet como en una Extranet ampliando con esto su campo de uso en un centro de trabajo.
- La información extraída de la Base de datos del sistema puede ser explotada de manera fácil y sencilla, obteniendo la toma de decisiones necesarias.
- El sistema ha sido desarrollado de forma escalar, de tal forma que cada empresa que lo utilice pueda agregar módulos de acuerdo a sus necesidades especificas.
- Al utilizar como medio de comunicación el protocolo TCP/IP, cualquier terminal que cumpla con los requisitos podrá tener acceso al sistema.

El sistema desarrollado en la presente tesis cumple con el objetivo trazado al inicio de la misma, que es la de registrar entradas y salidas de personal, así como la de visitantes, además permite el monitoreo de una manera ágil rápida y segura, esto se logro gracias a la utilización tecnologías Web de programación (como ASP, XML etc) y a dispositivos de identificación, en este caso Códigos de barras.

ANEXOS

ANEXO 1

Diccionario de Datos para el Sistema de control de acceso de personal en línea

TABLA	NOMBRE DEL CAMPO	TIPO DE DATOS	LONGITUD	PRECISIÓN	ACEPTA NULOS	VALOR PREDETERMINADO	LLAVE PRIMARIA	LLAVE FORANEA	DESCRIPCIÓN

- **Catálogo de Grupos (Cat_Grupo)**

Menu_Grupo	Id_Grupo	smallint	2	5			*		Identificador del Grupo.
Menu_Grupo	Nombre_Grupo	varchar	50	0	*				Nombre del Grupo

- **Catálogo de Menus (Cat_menu)**

Cat_menu	Id_menu	int	1	1			*		Identificador del menu
Cat_menu	Submenus_menu	bit							Submenu
Cat_menu	Id_submenu_menu	smallint	0	0			*		Identificador del submenu
Cat_menu	etiqueta_menu	varchar	50	0					Etiqueta del menu
Cat_menu	accion_menu	varchar	150	0					Acción del menu
Cat_menu	visible_menu	bit			*				Etiqueta para hacer visible o invisible una opción del menu
Cat_menu	Orden_menu	smallint	0	0	*				Orden en que se desplegará cada opción del menu

- **Catálogo de PCs (Cat_PC)**

Cat_PC	Id_PC	smallint	2	5			*		Identificador de la Computadora Personal (PC)
Cat_PC	Descripcion_PC	varchar	50	0	*				Descripción de la Computadora Personal (PC)
Cat_PC	IP_PC	varchar	15	0					Dirección IP de la Computadora Personal

									(PC) que accede al sistema
Cat_PC	Ustatus_PC	varchar	50	0					Estatus de de la Computadora Personal (PC)
Cat_PC	Fe_baja_PC	datetime	8	0					Fecha en que se dio de baja de la Computadora Personal (PC) asociada a una dirección IP.
Cat_PC	Fe_cambio_PC	datetime	8	0					Fecha en que se efectuó algun cambio al Catálogo de PCs

- **Catálogo de secciones (Cat_seccion)**

Cat_seccion	Id_seccion	smallint	2	5			*		Identificador de la sección
Cat_seccion	Clave	varchar	5	0					Clave de la sección a manera de alias ó descripción corta de la sección
Cat_seccion	Descripcion	varchar	50	0					Descripción de la sección
Cat_seccion	Id_PC	smallint	2	5				*	Identificador de la Computadora Personal o Cliente que se estará comunicando con el servidor de Web
Cat_seccion	Ustatus	varchar	1	0					El estatus de la sección ('A' Activa ó 'I' Inactiva)
Cat_seccion	Fe_baja	datetime	8	0	*				Fecha de baja ó en que se puso una sección con estatus de Inactiva
Cat_seccion	Fe_cambio	datetime	8	0		(getdate())			Fecha de cambio ó en que se efectuó alguna modificación en la Base de Datos para el Catálogo de secciones

- **Catálogo de Usuarios (Cat_usuario)**

Cat_usuario	Id_usuario	smallint	2	5			*		Identificador del usuario
Cat_usuario	Nombre_usuario	varchar	50	0					Nombre del usuario
Cat_usuario	Ape_pat_usuario	varchar	50	0					Apellido paterno del usuario
Cat_usuario	Ape_mat_usuario	varchar	50	0					Apellido materno del usuario
Cat_usuario	Sistema_usuario	bit	1	0					Sistema del usuario
Cat_usuario	Contrasena_usuario	varchar	1	0	*				Contraseña del usuario
Cat_usuario	Clave_usuario	varchar	8	0	*				Clave del usuario
Cat_usuario	CB_usuario	varchar	8	0					Código de Barras del usuario
Cat_usuario	Email_usuario	varchar	2	5					Correo electrónico del usuario
Cat_usuario	Telefono_usuario	varchar	5	0					Teléfono del usuario
Cat_usuario	Foto_usuario	image	16	0					Fotografía del usuario para su credencial
Cat_usuario	Direccion_usuario	varchar	100	0					Dirección o domicilio particular del usuario
Cat_usuario	Cargo_usuario	varchar	30	0	*				Cargo del usuario
Cat_usuario	Id_seccion_usuario	smallint	2	5	*				Identificador de sección a la cual tiene permitido acceder el usuario
Cat_usuario	Ustatus_usuario	varchar	1	0					Estatus del usuario
Cat_usuario	Fe_alta_usuario	datetime	2	5					Fecha de alta del usuario
Cat_usuario	Fe_baja_usuario	datetime	5	0					Fecha de baja del usuario
Cat_usuario	Fe_cambio_usuario	datetime	8	0					Fecha de cambio ó modificaciones al Catálogo de usuarios
Cat_usuario	Id_modificador_usuario	smallint	2	5				*	Identificador del usuario que realizó la modificación al Catálogo de usuarios
Cat_usuario	Tipo_usuario	varchar	1						Tipo de usuario ('V' Visitante, 'E' Empleado)

- **Tabla para registro de intentos de acceso fallidos que generan un mensaje de Error (Error)**

Error	Id_error	smallint	2	5				*	Identificador del menú
Error	Id_usuario	smallint	2	5				*	Identificador del grupo
Error	Id_seccion	int	4	10					
Error	Fe_acceso	datetime	8	0					

- **Histórico de accesos (Hist_acceso)**

Hist_acceso	Id_usuario_acceso	int	4	10				*	Identificador del usuario que accedió al sistema
Hist_acceso	Id_seccion_acceso	int	4	10				*	Nombre del Grupo
Hist_acceso	Hora_ent_acceso	datetime	8	0				(getdate())	Fecha y Hora en que un usuario entró al sistema
Hist_acceso	Hora_sal_acceso	datetime	8	0	*				Fecha y Hora en que un usuario salió del sistema

- **Tabla relación Menús con Grupos (Menu_Grupo)**

Menu_Grupo	Id_menu	smallint	2	5				*	Identificador del menu
Menu_Grupo	Id_grupo	smallint	2	5				*	Identificador del grupo

ANEXO 2

Descripción y organización del código

El código básicamente consta de archivos tipo ASP, HTML, ASA, JS, CSS, INC, XSL, GIF y JPG. Los archivos GIF y JPG corresponden a imágenes variadas del sitio, mientras que los demás archivos constituyen el núcleo del código principal del sistema.

Directorio raiz (sitio principal)	
ASP	Contiene el código ASP y HTML del sitio.
CSS	Contiene los estilos del sitio.
DLL	Contiene el componente *monitor.dll* así como el archivo *monitor.ini*
IMAGES	Contiene las imágenes del sitio.
INCLUDE	Contiene archivos - código de inclusión del sitio.
utilerias	Contiene códigos variados de apoyo para el sitio.
XSL	Contiene el código XSL del sitio.

- **Relación pantallas del sistema-código del sitio**

A continuación se describe cómo se conforman las pantallas a partir del código:

Pantalla	Archivos del sitio asociados
Acceso al sistema	index.html, acceso.html, logoArri.asp,logoIzq.html, VAL.ASP, RELOJ.JS, errorP.inc, errMnrP.xsl
Menú del sistema	tit_MonitorP.asp, MENU.ASP, MENUS.CSS, MENUS.JS, MENUS.XSL, comboMonitorP.xsl
Monitor del Personal	MonitorP.asp, MonitorP.xsl, FrMonitorP.html,, Empl_Seccion.asp, Empl_Seccion.xsl, Empls_Alerta.xsl, Empls_Alerta.asp, borraAlertas.asp
Accesos	AccesoP.asp, AccesoP1.html, AccesoP.html, accesoP.xsl, ErrorAcceso.inc, errMnrAcceso.xsl Visitas.asp,Visitas.xsl,Visita.asp, visita.xsl, act_visita.asp, CredencialV.asp, CredencialV.xsl
Empleados	empleados.asp, FrEmpleados.html, tit_empleados.asp, empleados.xsl, comboEmpleados.xsl
Mantenimiento a Empleados	Credencial.xsl,EMPLEADO.XSL,IDALIN.ASP,fotoEmpleado.asp,Credencial.asp,act_empleado.asp, EMPLEADO.ASP,
Catálogo de Computadoras	FrCatPCs.html,tit_PCs.asp, cat_PCs.asp, CatPCs.xsl, comboCatPCs.xsl
Mantenimiento a Catálogo de Computadoras	CatPC.xsl,act_PC.asp,cat_PC.asp
Catálogo de Secciones	cat_Secciones.asp, FrCatSecciones.html, tit_seccion.asp, CatSecciones.xsl, comboCatSecciones.xsl
Mantenimiento a Catálogo de Secciones	act_Seccion.asp, cat_Seccion.asp, CatSeccion.xsl
Multireportes	FrReportes.html, Reportes.asp,ReportesR.asp,ReportesP.txt, tit_Reportes.asp, Empl_Seccion.asp, comboTitReportes.xsl, Empl_Seccion.xsl, Reportes.xsl,ReportesR.xsl

Salir	SALIR.ASP
El sistema en general	GLOBAL.ASA,MONITOR.CSS,ERROR.INC,UTIL.ASP,UtilJs.js,errMnr.xsl

- **Descripción y organización del componente**

El componente cuenta con los siguientes métodos.

Método	**Descripción**
AccesoUsuario	Retorna la información básica del usuario que intenta ingresar a una *sección* con cierto *código de barras*
BuscaEmpleado	Busca al empleado que ingresó al sistema con cierta *clave*.
CambiaAtributo	Función que inserta un atributo en un documento XML.
ConsulEmpleados	Retorna la información de uno o más empleados.
ConsulJerarquias	Retorna las jerarquías o tipos de usuario del sistema.
ConsulPCs	Retorna la información de una o más PCs.
ConsulSecciones	Retorna la información de una o más secciones.
InsertXMLenXML	Función que inserta un documento XML en otro.
ObtenFotoEmpleado	Retorna la información de la fotografía del empleado.
ProcesaTabla	Función que procesa la información de los distintos catálogos del sistema.
Reportes	Retorna la información concerniente a los reportes del sistema.
UsuaXSecc	Retorna la relación de usuarios por sección.
ValidaUsuario	Retorna la información de configuración de menús del usuario en base a su clave y contraseña.
BorraAlertas	"Borra" el histórico de los alertas de intentos de acceso a secciones sin haber pasado por la entrada principal
ConsulErrorEntrada	Regresa una relación de los intentos de entrada a una sección sin haber entrado por la entrada principal
ErrorEntrada	Guarda un error cuando alguien intentó entrar a una sección sin haber entrado por la entrada principal
ConsulVisitas	Consulta a los visitantes

Y cuenta también con las siguientes propiedades:

Propiedad	**Descripción**
Xml	Contiene el resultado XML de la información que se regresa.

GLOSARIO

ActiveX	Conjunto de tecnologías de Microsoft que se aplican a diferentes campos del software, entre ellos la World Wide Web. Todas estas tecnologías tienen en común que están construidas sobre el Modelo de Objetos Componentes COM(siglas en inglés de Component Object Model).
ANSI	Siglas de American National Standards Institute, Instituto nacional de estándares norteamericano. Es una organización encargada de crear estándares para la industria de la computación. Con lo anterior, es posible generar productos de manera adecuada. ANSI aplica a software, aplicaciones eléctricas, protocolos de comunicación, así como a una gran cantidad de áreas técnicas.
Aplicación	Es la integración de componentes de software (para el envío o recepción de correos, para subir archivos a un servidor, para bajar archivos de un servidor, para generar gráficas a partir de datos estadísticos, etc), interfaces y reportes integrados en un mismo software.
Atributo	Una columna de una relación o tabla, hablando en términos de bases de datos.
ASP	Páginas Dinámicas cuyo código fuente es interpretado por un browser o navegador y que se ejecuta del lado del servidor de aplicaciones (Active Server Pages, por sus siglas en inglés). Es un Lenguaje de Programación para sitios web dinámicos que integra el uso de otros lenguajes inmersos en él: VBScript, JavaScript, HTML, XML, XHTML, CSS, Java, Visual Basic, entre otros. También permite la interacción con Bases de Datos relacionales y con componentes de software diversos.
Autenticación	Validación e identificación de personas utilizando mecanismos ya establecidos para ello. Autenticación por Clave de usuario y Contraseña, vía Código de Barras, etc.
Barra	Cualquiera de las líneas oscuras que componen el código.
Base de Datos	Organización sistemática de archivos de datos, para facilitar el acceso, la búsqueda y la puesta al día de los mismos. Para el presente Sistema utilizaremos una Base de Datos relacional.
Biométrica	Tipo de autenticación mediante la cual se reconocen ciertas características que son diferentes en cada ser humano, tales como huellas dactilares, patrones de voz, rangos de vasos sanguíneos en la retina, muñeca o mano, firmas, así como

patrones de escritura.

bps

Bits por segundo (bits per second, por sus siglas en inglés). La unidad de medida de la velocidad de transferencia de información,en dispositivos tales como el Módem. Por ejemplo, un Módem envía datos a 9600 bps, 14400 bps, ó 28800 bps.Esto indica la cantidad de bits transferidos a través de una línea telefónica en un segundo dado.

Browser

También conocido como navegador, es un software que permite interactuar con ciertos archivos para su visualización a través de la Internet, ejemplos de Browser son: Internet Explorer de Microsoft y Navigator de Netscape.

Campo

La representación física de un atributo en una base de datos.

Cliente/Servidor

La forma más efectiva de conectar 10 ó más computadoras dentro de una red de computadoras que comparten información entre sí. El Servidor es una computadora dedicada que controla todos los programas y periféricos en una red.El Cliente es cualquier computadora que necesariamente debe contar con software que le permita acceder a la información almacenada en el Servidor. Este tipo de configuración es económica, ya que el Servidor, que generalmente es más poderoso y más rápido que las computadoras Cliente, por lo que,en el momento de la transferencia de información, el trabajo en red es considerablemente mucho más fluido.

Código ASCII

Código estándar norteamericano para el intercambio de información. (American Standard Code for Information Interchange, por sus siglas en inglés) Es un estándar para la representación de letras, números y caracteres especiales, mediante 7 bits, hay también una versión con 8 bits de ASCII llamada ASCII-8. Por ejemplo, la letra A se representa como: 1000001.

Código de Barras

Imagen que consta de líneas (barras) y espacios que representa un juego de caracteres que pueden ser letras, números o una combinación de los dos. Se utilizan en Sistemas de Control de Inventarios, tarjetas de identificación, correo postal, identificación de códigos de productos, localización de personas, etc. Para leer el Código de barras se utilizan dispositivos lectores de Códigos de barras, los cuales utilizan bandas magnéticas o bien haces de luz láser dirigidos al Código en cuestión.

Coercitividad

Grado de resistencia de las bandas magnéticas a los campos magnéticos.

Coercitividad baja(LO-CO: Low Coercitivity, Baja coercitividad; en idioma inglés)	Para bandas magnéticas de baja densidad, habitual en las tarjetas de uso bancario, requiere una coercitividad de 300 Oersted. Muy apta para empresas provistas de lectores-grabadores.
Coercitividad alta(HI-CO: High Coercitivity, Alta coercitividad; en idioma inglés)	Para bandas magnéticas de alta densidad (desde 2540 hasta 4000 Oersted). De gran resistencia a campos magnéticos, y una vez gravada es prácticamente imposible su descodificación.
Contenido	Información dinámica o estática que se encuentra inmersa en una aplicación para Web.
Contraseña	También conocida como password, es un valor alfanumérico que permite o no el acceso a los usuarios al Sistema de identificación y control de acceso de personal en línea.
CSS	Hojas de estilo en cascada (Cascading Style Sheets, en idioma inglés) Conjunto de procedimientos que nos llevan a controlar distintos aspectos visuales y dinámicos de las páginas web, tales como fuentes, colores, márgenes y otros. Se constituye con un pequeño archivo que se vincula a una o más páginas, con el cual se consigue un aspecto similar para todas.
Chip	Nombre popular de un Circuito Integrado, el cual es un microcircuito compuesto de dispositivos interconectados que se integran en una sola pastilla de silicio.
Diagrama Entidad-Relación	Modelo conceptual de la Base de Datos de manera estructurada y gráfica, incluye una representación de la lista de dominios usados por la Base de Datos y algunas indicaciones visuales de las relaciones, atributos y entidades de la misma.
Dirección IP	Una dirección del protocolo de Internet de una computadora, un número que se divide en cuatro partes y que identifica al equipo en Internet. Es como el número de teléfono de la computadora.
Directorio virtual	Un directorio creado mediante herramientas de administración de sitios Web, y de manera análoga a como se generan los directorios desde el Explorador de Windows, así, dicho software nos permite generar directorios vistos únicamente vía un browser, así como organizar nuestro sitio Web de manera ágil y práctica.
DLL	Bibliotecas de enlace dinámico (Dynamic Link Libraries, por sus siglas en inglés) Aplicaciones cuyo código es invisible al usuario y que hace llamadas a procedimientos inmersos en este código, fue creada por Microsoft para obtener una ejecución más rápida de los procesos, dentro de una aplicación

o Sistema de información.

DOM — Modelo de Objetos de Documento (Document Object Model, por sus siglas en inglés). Es una especificación para interfases de programación que ha sido desarrollada por el consorcio de la telaraña de cobertura mundial(World Wide Web Consortium ,W3C; por sus siglas en inglés), la cual permite que un programador cree y modifique páginas con HTML, así como documentos XML. Tales documentos, podrán tener su contenido y datos ocultos dentro de cada objeto, procurando con ello, tener control en todo el documento. Como son objetos los documentos, pueden ir acompañados de procedimientos orientados a objetos denominados métodos. El DOM se vale de DHTML con la finalidad de aprovechar el comportamiento del browser con respecto a las páginas Web y a los elementos contenidos en ellas.

DTD — Definición de Tipos de Documento (Document Type Definition, por sus siglas en inglés).Un DTD es una definición especifica que sigue las reglas del Lenguaje de etiquetas estándar generalizado (SGML, por sus siglas en inglés). Un DTD es una especificación que acompaña a un documento e identifica la separación entre párrafos, encabezados. Esto implica que todo el contenido incluido en un documento se procese de acuerdo a un DTD, como es el caso de HTML. Para este último, el intérprete del DTD es el browser.

En Línea — Se refiere a la ejecución vía Internet a través de un Browser de una aplicación, justo en el momento en que la requerimos, desde el punto de vista del usuario.

Entidad — Cualquier cosa o ente sobre la que el sistema debe almacenar información o sobre la cual es posible su representación dentro de una base de datos

Esquema — La disposición física de las tablas de un sistema de bases de datos.

Extranet — Una aplicación corporativa con salida a otras corporaciones, es decir, es una Intranet con salida a Internet

Funcionalidad — Es lo que el usuario puede hacer en un sitio, como pujar por los artículos de las subastas o comprobar saldos bancarios o interactuar con una base de datos como ocurre en el presente Sistema.

Hipertexto	Significa que existen palabras seleccionadas en un documento, que establecen ligas a otros documentos que pueden estar ubicados en distintos servidores del mundo, donde en pantalla se muestran como si una página fuera la consecutiva de la anterior. Cada documento en hipertexto puede entrelazarse con múltiples textos, ya que cada conexión a otro documento puede realizarse a distintos lugares y donde toda esa información puede ubicarse en localidades muy distantes, el hipertexto se reconoce a diferencia del resto del texto porque está subrayado con distinto color, o por incorporar un número en paréntesis cuadrados.
HTML	Lenguaje de Etiquetas de Hipertexto(Hypertext Markup Language, por sus siglas en inglés).Lenguaje de programación de páginas Web creado por Timothy Burners Lee, que permite la navegación mediante un Browser entre páginas Web.
HTTP	Protocolo de Transferencia de Hipertexto (HyperText Transfer Protocol, por sus siglas en inglés). Protocolo utilizado para la transferencia de páginas o documentos Web.
Id de usuario	Es una cadena de caracteres que identifica al usuario y le permite, junto con una contraseña, ingresar o no a un sitio, cuando se utiliza el método de autenticación por Id y contraseña.
IIS	Servicios de Información en Internet (Internet Information Services, por sus siglas en inglés). Es una herramienta de Microsoft para la creación y administración de sitios Web.
Integridad de los datos	Las reglas utilizadas por una base de datos para asegurar que los datos son, si no correctos, al menos plausibles.
Integridad referencial	Las restricciones de integridad que aseguran que las asociaciones entre entidades siguen siendo válidas.
Interfaz	Es la "piel" de un sitio Web, que incluye botones, imágenes, diseño, etc, o sea, las piezas que ve el usuario y con las cuales interactúa.
Internet	Red de telecomunicaciones nacida en 1969 en Estados Unidos, a la cual están conectados millones de personas, organismos y empresas en todo el mundo (sobre todo en los países mas desarrollados), con trascendentes efectos sociales, económicos y culturales
Internet Explorer	Navegador o Browser para Web creado por la empresa estadounidense Microsoft. Es uno de los más difundidos por Internet.

Intranet Es una red propia de una organización, diseñada y desarrollada según los protocolos propios de Internet.

Puede tratarse de una red aislada, es decir, no conectada a Internet.

JavaScript Lenguaje para generación de scripts inmersos en páginas Web que pueden ejecutarse tanto del lado del Cliente como del Servidor y permiten efectuar validaciones, generar efectos e implementar interactividad con el usuario, en un entorno Web.

LAN Red de Área Local (Local Área Network, por sus siglas en inglés): Red de datos que le da servicio a un área geográfica de unos pocos kilómetros cuadrados; así pueden optimizarse los protocolos de señal de la red para llegar a velocidades de transmisión de hasta 100 Mbps (100 megabits por segundo).

Layers Los Layers son una de las aplicaciones de las Hojas de estilo en cascada que permiten variar el contenido de una página web, mediante el uso de HTML Dinámico, al generar capas o porciones de pantalla (Layers) que se desplazan en el browser de manera vertical u horizontal, así como sustituir un contenido por otro o sobreponer un contenido encima de otro. Los Layers pueden programarse de manera calendarizada, ósea, activarse en un momento dado, o bien, el usuario interactuar con ellos, como es el caso de los menús de opciones hechos con Layers.

Llave foránea Es una llave que existe como primaria en una tabla origen, es la referencia a dicha llave en una tabla detalle.

Llave primaria Es un identificador único que hace que exista relación entre tablas.

Menú Lista de comandos u opciones a disposición del usuario de un programa, con el objeto de que elija alguno de ellos.

Microprocesador Pastilla (chip) que contiene a la Unidad Aritmética Lógica (ALU), la Memoria de trabajo y la Unidad de Control de una computadora; el microprocesador es la Unidad de Procesamiento Central (CPU, por sus siglas en inglés) de una computadora

MODEM Abreviación de Modulador.Demodulador (MOdulator.DEModulator, en idioma inglés) Dispositivo electrónico que convierte datos de una computadora de forma que la transmisión de información sea vía telefónica. La conversión de digital a analógico es necesaria, ya que la línea telefónica transmite señales analógicas y las computadoras procesan información digital

Modelo de datos	La descripción conceptual de un espacio del problema en términos relacionales.
Parser	Programa que forma parte de un compilador, el cual recibe como entrada el Código fuente de un programa, en forma de instrucciones secuenciales, comandos interactivos en línea, etiquetas de HTML, o alguna otra interfase definida y reconocida por él. EL Parser se encarga asimismo de verificar que todo lo requerido por el programa se haya incluido.
PC	Computadora Personal (Personal Computer, en idioma inglés). Máquina de computación de tamaño sobremesa y de prestaciones cada vez más elevadas.
Protocolo	Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar estos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina-a-máquina o intercambios de alto nivel entre programas de asignación de recursos. Los protocolos "gobiernan" formatos, modos de acceso, secuencias temporales. Pueden ser normados (definidos por un organismo capacitado, como la CCITT o la ISO) o de ipso (creados por una compañía y adoptados por el resto del mercado).
Pruebas de usabilidad	Son pruebas objetivas realizadas a una interfaz para determinar la facilidad o dificultad que encuentren los usuarios para encontrar lo que buscan en un sitio Web.
Red	Es un sistema de hardware, software y canales de comunicación que conecta a diversos dispositivos.
Relación	En la teoría de Bases de Datos, es una construcción lógica que organiza los datos en filas y columnas
Sección	Es cada una de las ubicaciones físicas dentro de una institución o empresa en la cual se encuentra una persona.
Servidor Web	Es un sistema de cómputo que cuenta con software para la administración de servicios de Internet y a través del cual, es posible montar aplicaciones visibles desde un browser desde otras computadoras
SGML	Lenguaje de etiquetas generalizado (SGML. Standard Generalized Markup Language, en idioma inglés). Estándar para el cómo debe especificarse cada etiqueta y las etiquetas en conjunto HTML. Tal especificación es por sí misma una definición de tipos de documentos
Sistema	Es una aplicación informática que le permite al usuario interactuar de manera amigable con otros recursos como son:

	Bases de Datos, transferencia de información, modificación de la misma, etc.
Sistemas de identificación	Conjunto de métodos utilizados para la autenticación de los individuos y objetos, que se valen de medios magnéticos, ópticos, acústicos o registros impresos.
Sitio	Conjunto de archivos con contenido que se ejecuta en un browser y que en su mayoria es dinámico.
Sitio web público	Es aquél al que puede acceder cualquier usuario de Internet. Normalmente los cambios se efectúan en una máquina de desarrollo y los usuarios no los ven hasta que se hacen públicos.
SQL	Lenguaje de consulta estructurado(Structured Query Language, por sus siglas en inglés); es un lenguaje de base de datos. Se trata de un estándar - aunque distintos manejadores de bases de datos suelen presentar versiones ligeramente diferentes- pensado exclusivamente para crear o modificar las estructuras de una base de datos (tablas, vistas, índices, etc.) y agregar o modificar datos en ella. A su vez, SQL se utiliza para crear procedimientos almacenados (stored procedures, por su nombre en inglés) y desencadenadores (triggers, por su nombre en inglés).
SQL Server	Es un Sistema de Gestión de Bases de Datos creado por Microsoft y que permite crear, mantener y administrar Bases de Datos de mediana escala de crecimiento en los datos.
Tabla	La ejemplificación física de una relación en el esquema de la Base de Datos.
TCP/IP	Transmission Control Protocol/Internet Protocol o Protocolo de Control de Transmisión/Protocolo de Internet : Es la familia de Protocolos utilizados por Internet. Con TCP/IP, cada nodo o punto de red, está unido a la red mediante al menos una interfaz de red. Cada una de esas interfaces está perfectamente identificada por una dirección IP, en donde esta dirección es única por Computadora Personal. Con el objeto de ofrecer algo más adecuado a las necesidades de las aplicaciones, por encima de IP se ha desarrollado el protocolo TCP, el cual ofrece un mecanismo de comunicación basado en la idea de un canal fiable y bidireccional para el intercambio de octetos, no pierde datos, ni los desordena, y nos resuelve problemas de control de flujo de los que tambien adolece IP. Además, TCP es capaz de atender a varios usuarios (procesos) a la vez, manteniendo múltiples conexiones simultáneas.

Unicode

Estándar para la representación de texto y caracteres. Oficialmente se denomina Estándar Unicode para la representación de caracteres a nivel mundial(Unicode Worldwide Character Standard). Es un sistema para el intercambio, procesamiento y despliegue en pantalla de texto escrito e diversos idiomas del mundo moderno. Actualmente, Unicode contiene 34,168 caracteres codificados derivados de 24 idiomas. Estos caracteres cubren los principales idiomas del mundo.

VBScript

Lenguaje intérprete derivado de la sintaxis clásica de Visual Basic. Su origen, así como el propio origen de la herramienta de programación, aparece por primera vez dentro del producto Microsoft Word para Windows, recibiendo entonces el nombre WordBasic. Pero para que VB Script llegue a todos los rincones del mundo a través de la superautopista de la información(Internet), hace falta un vehículo adecuado: las páginas ASP.

WORM

Memoria de una sola escritura y de varias lecturas (Write Once, Read Many, por sus siglas en inglés) .Dispositivo para el almacenamiento de información que únicamente puede grabarse o escribirse información en él una sola vez. Una vez que se llena la memoria WORM, esta se vuelve de solo lectura y no puede ni modificarse ni borrarse. Lo anterior permite ter un medio de almacenamiento seguro, pues IThis has obvious advantages as far as security is concerned, in that once information is recorded it cannot be altered or added to in any way. Another advantage is that WORM files a información contenida en él no puede alterarse en ningún momento.

WWW

WWW o Web : Son las siglas de World Wide Web (Telaraña de cobertura mundial). Esta es una de las tantas sub-redes que posee Internet. Que se caracteriza por sus dos aplicaciones multimedia. Gopher y Http., que asemeja una telaraña, pues a medida que diveras instituciones públicas y privadas del mundo van adoptando esta tecnología, dicha red crece como si fuera una telaraña, pero de información

XHTML

Lenguaje de Etiquetas de Hipertexto Expandible(Extensible Hypertext Markup Language, por sus siglas en inglés) .Replantamiento de HTML 4.0 como aplicación de XML. Se dice que es expandible, ya que cualquiera que lo utilice puede inventar un conjunto de etiquetas e particular para un propósito en particular, con cual, XHTML se puede adaptar a cada aplicación e que se le utilice en particular, que incluye el cambio de apariencia de una página Web.

XML

eXtensible Markup Language o Lenguaje de Marcas expandible:
Es un lenguaje surgido a partir de HTML, mientras que este se preocupa por el aspecto de los datos, XML se preocupa por su significado, ya que podemos crear etiquetas propias que describan con precisión lo que deseamos saber.

BIBLIOGRAFÍA

Bibliografía

- ALONSO, José Miguel
  TCP/IP en UNIX
  Programación de aplicaciones distribuidas
  Alfaomega Grupo Editor, S.A de C.V.
  1999.

- DU MORTIER, Gustavo
  Bases de Datos con Visual Basic 6.0
  Microsoft Press
  2000.

- CHASE, Nicholas
  Active Server Pages 3.0
  Serie Práctica.
  Prentice Hall.
  España.
  2000.

- BARRERA PACHECO, Roberto Carlos
  Curso de Creación de Páginas Web
  Farmacéuticos MAYPO, S.A. de C.V.
  México.
  2001.

- CASTILLO GONZÁLEZ, Oriana Yuridia
  Curso de Introducción a Internet
  Farmacéuticos MAYPO, S.A. de C.V.
  México.
  2000.

- Revista Sólo Programadores
  Especial Monográfico No. 2.
  Tower Communications.
  Madrid, España.
  1994.

- GOLDFARB, Charles F.& Prescod, Paul
  Manual de XML
  Prentice Hall, Iberia, S.R.L.
  Madrid, España.
  1999.

- KAY, Michael
  XSLT Programmer's Reference.
  Wrox Press
  PROGRAMMER TO PROGRAMMER
  2000

- BENAGE, Don
  Building Enterprise solutions with Visual Studio 6
  Sams Publishing
  Estados Unidos de América
  1998.

- ERDEI, William H.
  Bar Codes. Design, Printing and Quality Control.
  Ed.McGraw-Hill, Inc.
  1993.

- DU MORTIER Gustavo
  Bases de datos en Visual Basic 6.0.
  Ed.Microsoft Press.
  México.
  2000.

- Diccionario de la Computación
  Inglés-español.
  Ed.Trillas.
  México.
  1996.

- LONG Larry
  Introducción a las computadoras y al procesamiento de información.
  Ed.Prentice Hall Hispanoamericana, S.A.
  México.
  1988.

- Sólo Programadores.
  La revista de programación en castellano.
  Especial monográfico No. 2.
  Tower Communications.
  España.
  1988.

- GONZÁLEZ. Alfons
  Visual Basic. Programación Cliente/Servidor
  Ed.Alfaomega.
  México.
  1999.

  KENDALL, Kenneth E.
  Análisis y Diseño de Sistemas
  Ed. Pearson Educación
  3era Edición
  México
  1997
- WILSON, Brian
  Sistemas: Conceptos, Metodologías y Aplicaciones
  Ed. Grupo Noriega Editores
  México
  1993

Referencia Electrónica

http://www.dimension-x.com/cf-bcsym2.htm
http://www.codifikar.com.ar/Inf_tipos.htm
http://www.mecsw.com/stdorg/orgs.html
http://www.abarcode.net/es/index.html
http://www.barmax.com
http://www.revistabarras.cl/barritas.htm
http://codigosdebarra.com/
http://www.fpress.com/revista/num9603/mar96.htm
http://centros5.pntic.mec.es/cpr.de.aranjuez/foro/circo/codigo.html
http://www.idsys.es/capa1_1.htm
http://www.codigo.com.ar/boletines/boletin_16/b_16_07.htm
http://www.puntolog.com/foro/buzon/messages/5590.htm
http://www.cybra.com/glossary.htm
http://www.ceyal.com.ar/servicios/servicioschentes.htm
http://www.barmax.com/shoppingE/articulo_22.htm
http://www.amece.com.mx
http://www.area.com.mx/bar_code/
http://www.ast-atis.com.es/es-ID2.htm
http://www.schillig.com.ar/control_de_accesos_fr.htm
http://www.net-research.net/swen/biometri1.htm
http://neutron.ing.ucv.ve/revista-e/No6/Olguin%20Patricio/SEN_BIOMETRICOS.html
http://www.planeta-redvista.com.ar/abril99/adentro.htm
http://www.kimaldi.net/es/docs/products.php?filt=6
http://www2.ing.puc.cl/~ing/ed429/sistemas_biometricos.htm

http://www.insys.com.mx/biometria/lectores.htm
http://www.salvador.edu.ar/molina.htm
http://www.geocities.com/gcataneo/tarjetas.htm
http://www.capta.com.mx/folletos/etime.htm
http://www.genera.cl/Credenciales.htm
http://www.handheld.com/
http://www.programacion.net/html/xml/htmdsssl/capitulo1/capitulo1.htm
http://www.xml.com/pub/a/98/10/guide0.html
http://www.tejedoresdelweb.com/avanzado/introduccion_xml/index.htm
http://www.microsoft.com/windows2000/en/server/iis/default.htm?/htm/asp/aspguide.htm
http://www.w3.org/Style/CSS/
http://www.lavariable.com/tutoriales/css/INDEX.asp
http://www.w3.org/TR/REC-CSS1
http://www.arachnoid.com/lutusp/dll_article.html
http://dll.yaroslavl.ru/
http://www.itpapers.com
http://www.openconsult.com/whitepapers/extranets.rtf
http://www.microsoft.com/windows2000/en/server/iis/
http://www.programacion.net/html/xml/htmdsssl/capitulo1/capitulo1.htm
http://www.xml.com/pub/a/98/10/guide0.html
http://www.w3.org/Style/XSL/
http://www.w3.org/TR/xslt
http://www.w3.org/TR/xpath
http://www.w3.org/TR/xlink/
http://www.w3.org/Style/XSL/WhatIsXSL.html
http://wdvl.internet.com/Authoring/Languages/XSL/Quickly/quick1_1.html
http://www.programacion.net/html/xml/htmdsssl/capitulo1/capitulo1.htm
http://www.xml.com/pub/a/98/10/guide0.html
http://www.tejedoresdelweb.com/avanzado/introduccion_xml/index.htm
http://wdvl.internet.com/Authoring/Languages/XSL/Quickly/quick1_1.html
http://www.dundas.com
http://www.amece.com.mx/f_codigo.html
http://www.vectorda.com/hardware/tarjetas.htm
http://www.fortunecity.es/arcoiris/tarot/572/tar_mag.html
http://www.elektronica.com.ar/Tarjetas.html
http://www.akrocard.com/bmycodabar.htm
http://www-ni.laprensa.com.ni/archivo/2001/mayo/29/informatica/articulos/articulos-20010529-01.html
http://www.aim-mexico.com/
http://psasecurity.com/spanish/psaaccesscontrol.html
http://www.poptel.org.uk/mante/glossary/g186.htm
http://www.cknow.com/ckinfo/acro_e/eeprom_1.shtml
http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci213918,00.html
http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212749,00.html
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213800,00.html
http://whatis.techtarget.com/definition/0,,sid9_gci214201,00.html
http://whatis.techtarget.com/definition/0,,sid9_gci213250,00.html

http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci213550,00.html
http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci213404,00.html
http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci212418,00.html
http://whatis.techtarget.com/definition/0,,sid9_gci213910,00.html
http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci212022,00.html
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213800,00.html