Universidad Nacional Autónoma de México
Facultad de Ingeniería

Sistema de administración de inventarios de equipos y usuarios e incidentes de seguridad para un ISP

Tesis

que para obtener el título de Ingeniero en Computación presentan

Acosta Dionicio Jorge

Arreola Nava Oscar

Galicia Benhumea Jorge Alberto

Ortega Rodríguez Manuel Alejandro

Director de tesis: M. I. Juan Carlos Roa Beiza

México, D.F. Diciembre 2004

Agradecimientos

Esta tesis la dedico a mi esposa Tere e hijos Alberto y Omar en reconocimiento a la tolerancia y paciencia que me brindaron durante el tiempo que destine para la realización de esta.

Agradezco a toda mi familia, a mis hermanos, a mi mamá Rosita y a mis suegros por la compañía y apoyo que me brindan. Se que cuento con ellos siempre.

Agradezco a Dios por llenar mi vida de dicha y bendiciones.

Por último y de manera muy especial, la culminación de este esfuerzo está dedicada a mis Padres Vicky y Jorge, a quienes agradezco de todo corazón por su amor, cariño y comprensión. En todo momento los llevo conmigo.

Jorge A. Galicia Benhumea

Agradecimientos

A Dios:

Por permitirme llegar hasta este momento de mi vida.

A mis padres:

Por la educación que me han dado, pero sobre todo por sus enseñanzas, porque a través de ellas he aprendido a conducirme con gratitud, honestidad y sencillez.

A mi esposa y a mi hija:

Por estar conmigo siempre y apoyarme en las decisiones y logros más importantes de mi vida.

A mis hermanos:

Por compartir conmigo los buenos y malos momentos.

Manuel Alejandro Ortega Rodríguez

ÍNDICE

INTRODUCCIÓN XI

CAPÍTULO I. POLÍTICAS DE LA EMPRESA

1.1 Misión del ISP 3
1.2 Misión del Departamento de Seguridad del ISP 7
1.3 Políticas de la empresa que involucran al área de seguridad 13
1.4 Procedimientos actuales por el Área de Seguridad para el inventario de equipos y usuarios, y el seguimiento de incidentes de seguridad 20
1.4.1 Procedimientos de manejo y tratamiento de reportes de incidentes de seguridad 21
1.4.2 Inventario de equipos de red que constituyen la infraestructura de la empresa 25
1.4.3 Inventario de usuarios que tienen acceso a la infraestructura de red 26
1.4.4 Notificaciones 28

CAPÍTULO II. TEORÍA BÁSICA

2.1 Bases de datos relacionales 31
2.2 SQL Server 2000, características, ventajas y desventajas 37
2.3 Visual Basic 6.0, características, ventajas y desventajas 42
2.4 HTML y ASP, características, ventajas y desventajas 48
2.5 Sistema operativo Windows 2000 Server y Windows XP 53
2.6 Redes y comunicaciones 57
2.7 Seguridad 61

CAPÍTULO III. PLANTEAMIENTO DE PROBLEMA Y PROPUESTA DE SOLUCIÓN

3.1 Problemática actual 71
3.2 Requerimientos generales y particulares 78
3.3 Recopilación y análisis de la información 89
3.4 Identificación del problema 96
3.5 Opciones de solución y selección de la óptima 106

CAPÍTULO IV. DESARROLLO E IMPLEMENTACIÓN DEL SISTEMA

4.1 Aplicación de la metodología elegida 115
4.1.1 Diagrama de contexto 115
4.1.2 Diagrama de flujo 121
4.1.3 Diccionario de datos 125
4.1.4 Diagrama Entidad-Relación 131
4.1.5 Normalización 133
4.2 Diseño y construcción del Back-End 140
4.3 Diseño y construcción del Front-End 158
4.4 Pruebas e implantación del sistema 179
4.5 Factibilidad técnica y operativa 187
4.6 Obtención de reportes 191

MANUAL DE USUARIO

1. Descripción general 203
2. Acceso al sistema 204
3. Administración de usuarios 205
4. Administración de equipos de red 209
5. Notificaciones de seguridad 211
6. Funciones del menú principal 214

7. Incidentes de seguridad 217
8. Bitácoras 218
9. Búsquedas 219
10. Reportes 220
11. Opciones 220

MANUAL TÉCNICO

1. Descripción General 225
2. Respaldo de la base de datos 226
3. Restauración de un respaldo de la base de datos 228
4. Automatización de respaldos 229
5. Control del servicio de SQL Server 229

CONCLUSIONES 231

BIBLIOGRAFÍA 235

INTRODUCCIÓN

La licenciatura en Ingeniería en Computación impartida por la Universidad Nacional Autónoma de México, en su Facultad de Ingeniería proporciona una formación tecnológica enfocada al desarrollo de soluciones informáticas que satisfacen a los distintos requerimientos del mercado, de acuerdo a las necesidades de cada empresa.

Como una aplicación práctica de los conocimientos adquiridos en la carrera, se presenta este trabajo, en el cual se hace un análisis detallado y se proporciona una solución para el desarrollo de una aplicación con arquitectura cliente servidor encargada de administrar los inventarios de equipos y cuentas de usuario registrados en la infraestructura de red de un Proveedor de Servicios de Internet (ISP, por sus siglas en inglés), así como un control de los casos de incidentes de seguridad que son reportados por las diferentes entidades, dándose una solución a cada uno de ellos.

El desarrollo del sistema se plantea en cuatro secciones o capítulos en los cuales se abordan cada uno de los aspectos principales, desde el inicio del análisis hasta las pruebas y reportes de operación del sistema.

En el capítulo I, se proporciona un panorama general de la empresa en cuanto a su operación, su misión, los servicios que ofrece, cómo los ofrece y sus políticas. También se abordan aspectos de la operación de su departamento de seguridad, al cual va dirigido el sistema, así como las operaciones que esta área realiza antes de su puesta en marcha.

En el capítulo II se proporcionan todos los aspectos teóricos necesarios para el desarrollo, los cuales van desde las características principales de las bases de datos relacionales, hasta las características y ventajas de las herramientas de software a

utilizar, tales como sistemas operativos, bases de datos, lenguajes de programación y herramientas para desarrollo Web.

En el capítulo III se presenta todo el estudio realizado a los requerimientos del área de seguridad del ISP, en donde se expone detalladamente la operación del departamento antes de que el sistema sea desarrollado, ubicando los puntos críticos y haciendo énfasis en la forma en que serán solucionados por la aplicación una vez que ésta quede implementada.

En el capítulo IV, se detalla la construcción de la aplicación en su totalidad, involucrando todo el desarrollo desde la instalación de las herramientas de software utilizadas y la preparación y puesta a punto de las partes de Back-End y Front-End del sistema, hasta la ejecución de pruebas, estudios de factibilidad operativa y reportes.

Para finalizar este trabajo se incluyen los manuales de usuario y técnicos que se utilizarán a lo largo de la operación del sistema.

CAPÍTULO I
POLÍTICAS DE LA EMPRESA

1.1 MISIÓN DEL ISP

Misión

Ser una empresa líder en telecomunicaciones, que proporcione a sus clientes soluciones integrales de gran valor, innovadoras y de clase mundial, a través del desarrollo humano, y de la aplicación y administración de tecnología de punta.

Visión

Consolidar el liderazgo de la empresa, expandiendo su penetración de servicios de telecomunicaciones en todos los mercados posibles, para situarse como una de las empresas de más rápido y mejor crecimiento a nivel mundial.

Solución Integral

La empresa forma parte de un paquete de soluciones integrales para todos los sectores del país. El liderazgo de la empresa se refleja en una poderosa gama de servicios, desde equipo y enlaces privados hasta el acceso a Internet, la red pública de datos de mayor velocidad y más amplia cobertura para cubrir las necesidades de los sectores Turismo, Educación, Salud, Servicios, Industria, Finanzas y Gobierno.

Socios Tecnológicos

La empresa integra en sus soluciones los productos de mayor calidad y mejor rendimiento del mercado. La obligación y meta de la empresa consiste en buscar y ofrecer a los clientes la mejor alternativa costo beneficio para la integración de sus redes. La estrecha relación de la empresa con sus proveedores asegura a los clientes la tranquilidad que esperan al confiar su red en el funcionamiento de los equipos seleccionados por la empresa. Además de ello, la empresa tiene el respaldo de sus socios tecnológicos durante las veinticuatro horas del día, los trescientos sesenta y

cinco días del año, para que, en caso de cualquier contingencia, el cliente cuente siempre con el soporte necesario.

Consultoría y diseño de redes

La empresa cuenta con un grupo de consultores expertos en varias plataformas tecnológicas de voz, datos e imagen. Los clientes cuentan con el apoyo de este grupo experto para el diseño y/o la optimización de su red de transporte de información. El deseo es proporcionar las herramientas necesarias para que su negocio esté siempre a la vanguardia en comunicación de datos, acceso a Internet, videoconferencias y cualquier otro avance en la industria que pueda ser de beneficio para su negocio.

Servicios Profesionales de soporte

La empresa ofrece una amplia cartera de servicios de soporte y asistencia técnica especializada para la instalación, el mantenimiento y la puesta a punto de sus redes de voz, datos e imagen.

Servicios

Los servicios básicos que se ofrecen para formar este tipo de redes, son los siguientes:

Servicios Virtuales Permanentes. Servicio a través del protocolo de enrutamiento **IP** (Internet Protocol – Protocolo de Internet) y comprende las modalidades IP Dedicado e IP Conmutado.

La infraestructura de red cuenta además con servicios de valor agregado que permiten ofrecer alternativas de comunicación a través de su red de transporte basada en tecnologías de conmutación de paquetes de datos. Los Servicios de Acceso a Redes de Información comprenden el acceso y la conexión a diferentes redes, así como a nuevas aplicaciones, entre las que se ofrece el siguiente servicio:

Servicio IP Dedicado

El Servicio IP Dedicado ofrece una alternativa para las diferentes necesidades de los usuarios corporativos que requieren de una conexión a la red mediante el uso del protocolo de datos IP. Los servicios de transporte de datos IP que ofrece la empresa representan una solución adecuada para que los usuarios puedan transportar la información de sus aplicaciones e Intranets de una forma confiable y segura.

El Servicio IP Dedicado está basado en el conjunto de protocolos **TCP/IP** (Transfer Control Protocol / Internet Protocol – Protocolo de Control de Transferencia / Protocolo de Internet), los cuales ofrecen una facilidad de acceso a la red que consiste en un enlace que se establece desde la localidad del usuario al nodo más cercano de la red de la empresa, el cual es conocido como el acceso de datos y que cuenta además con un puerto en el nodo correspondiente.

Este servicio se ofrece en forma permanente en donde el acceso digital se entrega a través de la implantación de un enlace. Como parte integral de la solución completa, este servicio normalmente se instala en los nodos corporativos centrales de las redes de las corporaciones, con el objetivo de ser el punto de entrada de los datos enviados por usuarios remotos que acceden a la red vía el servicio IP Conmutado para realizar sus aplicaciones de datos en los servidores o procesadores centrales, **host** (huésped).

Servicio IP Conmutado

De la misma manera, el Servicio IP Conmutado ofrece una alternativa para las diferentes necesidades de los usuarios corporativos que requieren de una conexión temporal o esporádica a la red para sus nodos o usuarios remotos mediante el uso del protocolo de datos IP. A través de este protocolo se ofrece una solución adecuada para los usuarios, que cuentan con una sola computadora personal o laptop y puedan

transportar la información de sus aplicaciones y obtener acceso remoto a sus Intranets de una forma confiable y segura.

En el Servicio IP Conmutado la conexión a los servicios que ofrece la empresa se hace a través de modems utilizando una línea analógica de la red pública conmutada de Telmex, en donde la empresa proporciona un solo punto de conexión por nodo disponible a nivel nacional a través de un número telefónico establecido. Como parte integral de la solución completa, este servicio se emplea en conjunto con el servicio IP Dedicado para que los usuarios remotos establezcan su conexión con el servidor o procesador central.

Servicio Internet Empresarial

La infraestructura de red ofrece servicios complementarios que brindan un valor agregado tales como el acceso a redes de información para usuarios corporativos, comerciales y residenciales. Entre las redes más importantes a nivel mundial se encuentra la red Internet, a través de la cual la empresa mantiene una conexión de alta capacidad ofreciendo con esta infraestructura el acceso, la conexión y el transporte de información para dichos usuarios.

El servicio empresarial o para **ISP** (Internet Service Providers - Proveedores de Servicios de Internet) se conoce como Internet Empresarial y se ofrece en la modalidad permanente y comprende el acceso local y la interconexión con la red dorsal basada en ruteadores que se mantiene en operación exclusivamente para permitir el acceso y transporte de los servicios de Internet.

Los servicios que ofrece la empresa a sus clientes son, además de la conectividad, el anuncio de sus redes hacia Internet, permitiendo que cualquier usuario en el mundo pueda acceder a ellas.

1.2 MISIÓN DEL DEPARTAMENTO DE SEGURIDAD DEL ISP

El Departamento de Seguridad de Red es el área encargada de definir, implantar y administrar los esquemas de seguridad para las redes, mediante la planeación, implantación y seguimiento de políticas y procedimientos de operación que se alineen con las políticas definidas por la empresa, para asegurar la integridad y confiabilidad de los servicios, recursos y sistemas que emplean o proporcionan dichas redes.

La Administración de Seguridad es el área responsable de tomar las medidas para asegurar la integridad de los recursos, dispositivos e información con que cuentan la red.

Panorama general de la Administración de Seguridad

La Administración de Seguridad es una disciplina perteneciente a la Administración de Operaciones, la cual es responsable de asegurar que la operación de los servicios de TI (Tecnología de Información) sea ejecutada de acuerdo con los estándares y las mejores prácticas de trabajo acordados en la organización. La calidad de los servicios debe cumplir con los Acuerdos de Niveles de Servicio negociados con los clientes.

Las funciones de la Administración de Operaciones son:

- Administrar las instalaciones de la infraestructura de TI.
- Administrar los componentes de la infraestructura de TI.
- Ejecutar los servicios de TI.
- Monitorear el estado de los componentes de la infraestructura.
- Identificar incidentes y notificar alertas apropiadas.
- Mejorar continuamente la operación.
- Generar reportes de administración.

Para lograr toda esta gama de funcionalidades, la Administración de Operaciones se apoya en diversos subprocesos, con los que busca cubrir todos los aspectos operacionales de una organización. Los principales subprocesos de la Administración de Operaciones son:

- Administración de Aplicaciones.
- Administración de **LAN** (Local Area Network – Red de Área Local) / **WAN** (Wide Area Network – Red de Área Amplia).
- Administración de IP.
- Administración de Bases de Datos.
- Administración de Salidas (output).
- Administración de Respaldos y Almacenamiento.
- Calendarización de Producción y Procesamiento.
- Monitoreo de Desempeño y Afinación.
- Control y Seguridad de Acceso.
- Detección y Notificación de Eventos.

Contenida dentro de la Administración de Operaciones, la Administración de Seguridad es una disciplina que permite ofrecer los servicios de seguridad de red contra amenazas de seguridad de la misma y consisten en ocho elementos principales:

- Control de acceso de conexión.
- Autenticación de conexión.
- Autenticación de origen de datos.
- Integridad.
- Confidencialidad.
- No rechazo del servicio.
- Mejora continua.
- Administración de la información de los cuatro puntos anteriores.

Antecedentes de la Administración de Seguridad

La Administración de Seguridad es una disciplina que permite manejar y controlar la seguridad que se requiere dentro de la organización a través de los servicios de TI. Ayuda no sólo a minimizar el impacto y el riesgo que implica proveer los servicios de telecomunicaciones, además toma el control de todo cambio o intrusión realizada sin el conocimiento de los administradores y permite detectar y evitar futuras fallas en los servicios y perdidas de información o acciones de sabotaje.

Además, la Administración de Seguridad es también la disciplina responsable de definir y vigilar el cumplimiento de las políticas de acceso a los recursos del negocio, incluyendo servicios, redes, elementos tecnológicos e información.

Misión de la Administración de Seguridad

Asegurar que los recursos sean utilizados y accedidos sólo por las personas que defina el negocio de acuerdo con los estándares y las mejores prácticas de trabajo acordados en la organización y cumpliendo los acuerdos de niveles de servicio negociados con los clientes.

Objetivos Generales de la Administración de Seguridad

- Alinear la Administración de Seguridad con los requerimientos del negocio de la organización.
- Ejecutar los servicios de seguridad de acuerdo a las mejores prácticas definidas en la organización.
- Alinear la Administración de Seguridad a la estrategia tecnológica.
- Cumplir con la calidad de los servicios negociados en los Acuerdos de Niveles de Servicio.
- Mejorar continuamente la Administración de la Seguridad.

Proceso de Administración de Seguridad

En la tabla 1.2.1 se describen las actividades del Proceso de Administración de Seguridad, la entrada que alimenta dichas actividades y la salida que se espera recibir como mínimo en cada una de ellas.

Actividad	Descripción	Entrada	Salida
Definir estrategias de seguridad para tecnología.	Se establecen las estrategias de seguridad para el ambiente propio de la red.	Conocimiento del ambiente y la infraestructura propia de la red y de sus clientes.	Conocimiento real y actualizado, del ambiente y la infraestructura propia de la red y de sus clientes.
Definir acciones de recuperación y contención de seguridad.	Se definen las acciones que se seguirán en cualquiera de las dos posibilidades: recuperar y contener.	Conocimiento real y actualizado, del ambiente y la infraestructura propia de la red y de sus clientes.	Acciones que se llevarán a cabo al momento de que se presenten incidentes de seguridad.
Aplicación de estrategia tecnológica y su comunicación.	Se aplican las estrategias definidas y se comunican a todas las áreas para estandarizar la seguridad en la red.	Acciones establecidas que se llevarán a cabo después de detectado un incidente de seguridad.	Se aplica la estrategia tecnológica y se comunica a los administradores y operadores de la red.
Revisión de alarmas de seguridad de clientes.	Se revisan las alarmas de seguridad para definir posibles incidentes en los enlaces de los clientes.	Comunicación de la aplicación de la estrategia.	Parámetros de las alarmas establecidas en los servicios a los clientes.
Investigación de uso indebido de servicios de la red.	Se verifica el uso apropiado o no, de los servicios prestados a los clientes o sus enlaces.	Resultado del análisis de los patrones de uso del cliente con respecto al uso actual.	Se determinan si el cliente ha hecho uso indebido de los servicios contratados.

Tabla 1.2.1 Administración de seguridad.

Actividad	Descripción	Entrada	Salida
¿Se detectó incidente?	Se verifica si se trata de un incidente de seguridad.	• Resultado del análisis de los patrones de uso del cliente con respecto al uso actual. • Se determinan si el cliente ha hecho uso indebido de los servicios contratados.	• (Si) Se procede a recopilar la información que determina la aparición del incidente de seguridad. • (No) Información que concluye que no se presentó incidente de seguridad.
Registro de incidente de seguridad.	Se registra el incidente de seguridad a través de la Administración de Incidentes.	Información que determina la aparición del incidente de seguridad.	Registro del incidente de seguridad en la Administración de Incidentes.
Notificación de cierre de incidente.	Se notifica a la Administración de Incidentes que se cierra el incidente de seguridad.	Estado final de los permisos y perfiles del cliente, posterior a la detección del incidente de seguridad.	Notificación a la Administración de Incidentes de la resolución del incidente de seguridad.
Recibe notificación.	La Mesa de Ayuda recibe la notificación de cierre del incidente de seguridad.	Notificación a la Administración de Incidentes de la resolución del incidente de seguridad.	• Actualiza la Base de Datos de Conocimiento de la Administración de Incidentes. • Notifica al cliente/usuario en caso de ser necesario.
Revisión de alarmas de seguridad de redes.	Se lleva a cabo una revisión periódica de las alarmas establecida.	Información que concluye que se presento incidente de seguridad.	Revisión final de las alarmas establecidas y de su posible actualización o modificación.

Tabla 1.2.1 Administración de seguridad (continuación)

Actividad	Descripción	Entrada	Salida
Manejo de permisos o perfiles de administración de la red.	Se administran los permisos y/o perfiles del operador o administrador en cuanto a su uso de la red.	Revisión final de las funciones establecidas por área y de su posible actualización o modificación.	Modificación de permisos y perfiles de usuarios.
Investigación de uso indebido de la red por los operadores	Se analiza el posible uso indebido de los servicios de red.	Resultado del análisis de los patrones del uso interno de la red y sus servicios, además de alarmas, perfiles y permisos.	Se determinan si administradores y/u operadores han hecho uso indebido de los servicios de la red
Protección del almacenamiento de datos de configuración de red y elementos.	Se llevan a cabo las acciones definidas para proteger la información de la red y sus elementos.	Resultado de las acciones llevadas a cabo para establecer el nivel de seguridad óptimo.	Ajuste a la protección y respaldo de los datos de la red y elementos.
Asignación de incidente.	La Administración de Incidentes asigna a la Administración de Seguridad, los incidentes que se reporten a Mesa de Ayuda.	Recepción de datos y registro de un incidente de seguridad, recibidos por la Mesa de Ayuda.	Asignación a la Administración de Seguridad del incidente registrado.

Tabla 1.2.1 Administración de seguridad (continuación)

1.3 POLÍTICAS DE LA EMPRESA QUE INVOLUCRAN AL ÁREA DE SEGURIDAD

Seguridad

- Las Políticas de seguridad son aplicables a todas las unidades de negocio de la empresa, a sus empleados regulares y empleados no regulares tales como temporales, por honorarios, contratistas, proveedores y consultores. Estas Políticas se refieren a toda la información sin tomar en cuenta la forma, ni el formato.

- El Departamento de Seguridad de Red deberá preparar, mantener y distribuir uno o más manuales de seguridad de la información que describan en forma concisa las políticas y procedimientos de seguridad.

- Con objeto de difundir y capacitar al personal en aspectos de seguridad, se hace necesario el preparar un programa de concientización dirigido a los diferentes niveles organizacionales de la empresa.

Organización de la seguridad

- Se designa como entidad de normatividad y regulación de asuntos de seguridad de la información al Departamento de Seguridad de Red.

- La responsabilidad para dictar las políticas de la seguridad de la información estará en función de la estrategia de negocio de la empresa.

- La Subgerencia de Seguridad de Red es la entidad responsable de recibir y proponer las políticas, lineamientos estándares y procedimientos para ser aplicados a todos los niveles de la empresa.

- El Departamento de Seguridad de Red deberá proveer toda la dirección y apoyo técnico en seguridad que sea necesario para asegurar que la información de la empresa quede protegida adecuadamente minimizando la exposición a los riesgos.

- Deberá existir un perfil para cada rol dentro del Proceso de Administración de la Seguridad, en donde se definan las funciones y responsabilidades asociadas con el rol. Los roles definidos son Administrador de Seguridad y Operador de Seguridad.

- Todo el personal que se dedica a desarrollar actividades relacionadas con la administración de la seguridad deberá pertenecer a El Departamento de Seguridad de Red.

- El personal de El Departamento de Seguridad de Red deberá mantenerse actualizado en los avances tecnológicos en seguridad informática.

- Las actividades de administración de seguridad que sea necesario realizar en localidades descentralizadas, en las que no se cuente con personal de seguridad, serán realizadas por un recurso local al cual se le dará la responsabilidad de seguridad en esa localidad, con apego a las políticas corporativas.

- El Departamento de Seguridad de Red deberá definir un procedimiento de verificación para que en la adquisición de los nuevos equipos o nuevas tecnologías, éstos cuenten con un adecuado nivel de seguridad y sean integrados a la estrategia de seguridad.

- Los contratos de servicios con terceros, deberán contener cláusulas de seguridad que especifiquen claramente las responsabilidades de los prestadores de servicio, en lo referente a seguridad.

Responsabilidad del personal en seguridad de información

- Se incluirán dentro de las descripciones de puestos, las responsabilidades relativas a la seguridad de los activos dentro de la organización, y el cumplimiento de los procedimientos de seguridad.

- Las responsabilidades para la seguridad de la información día a día es de todos y cada uno de los usuarios y empleados de la empresa.

- Todos los empleados regulares, eventuales y terceros deberán firmar el acuerdo de desempeñar su trabajo conforme a las políticas y procedimientos mencionados.

- Todos los empleados deberán firmar un acuerdo para la seguridad informática y a intervalos regulares de tiempo refrendar su compromiso por cumplirlo. El acuerdo requerirá que el empleado reconozca que la violación de las políticas, reglas o procedimientos, será causa para tomar acciones disciplinarias que pueden llegar al despido.

- Se establecerá un programa de concientización de seguridad dirigido a todo el personal, con respecto a la importancia de los procesos de seguridad de la información en función del logro de los objetivos de negocio. Las políticas y los procedimientos explícitos de seguridad serán documentados y dados a conocer.

- La mesa de Ayuda o Help Desk cuando sea informado que algún software no esta funcionando de acuerdo a las especificaciones, y sospeche que se deba a un software malicioso, deberá reportarlo al Departamento de Seguridad de Red (incidentes).

- En caso de cometerse una violación a las políticas de seguridad de red, se hará un seguimiento en el que estarán involucradas las áreas de auditoría, recursos

humanos y legal hasta su completa aclaración llevándose a cabo las acciones disciplinarias que ameriten para el empleado que haya realizado la violación.

Control de acceso al sistema

- Toda persona que requiera acceder a los sistemas de cómputo deberá contar con una clave de usuario personalizada.

- Todos los recursos de los sistemas serán protegidos por los principales programas de seguridad. Dentro de la funcionalidad con que se debe contar para éstas herramientas de protección de acceso, están las de notificación en caso de ser detectada alguna violación de seguridad. Los recursos de cómputo que atienden a múltiples usuarios deberán, por lo tanto, ser capaces de:

    - Identificar y verificar la identidad y si es necesario conocer hasta la identificación y localización de la terminal o estación de trabajo de cada usuario autorizado.
    - Se deberá registrar los accesos exitosos y fallidos al sistema.
    - Proveer un sistema de administración de claves de acceso que asegure la calidad de las mismas.
    - Se deberá restringir en caso de ser necesario, el tiempo de conexión de los usuarios.

- Deben establecerse controles que prevengan el acceso no autorizado a la información. Un proceso de monitoreo se deberá establecer con el fin de registrar intentos de acceso no autorizados a los recursos protegidos.

  El acceso a los servicios de cómputo deberá ser controlado por medio de un procedimiento de registro que contemple dar de baja usuarios inexistentes. El procedimiento de registro de usuarios deberá contemplar los siguientes elementos:

- Se verificará que el usuario tenga la autorización del dueño de la información para accederla.
- Se verificará que los accesos concedidos al usuario son congruentes con sus responsabilidades y con los objetivos del negocio.
- Se entregará al usuario por escrito los accesos concedidos y se deberá obtener la firma de éste.
- Asegurar que no se proporciona el acceso a los servicios hasta que el procedimiento de autorización ha terminado.
- Mantener un registro formal de todas las personas registradas para usar los servicios.
- Dar de baja los usuarios que han cambiado sus responsabilidades.
- Establecer un procedimiento para aquellos empleados que son dados de baja por cualquier motivo, Recursos Humanos informará al área de seguridad para cancelar en forma inmediata todo tipo de acceso a los recursos de TI (Tecnología de Información).
- Periódicamente se deberá verificar que no existen usuarios que han dejado de laborar en la empresa.

- Todos los sistemas de cómputo y sistemas de red deberán incluir herramientas automatizadas suficientes, para apoyar la administración de la seguridad. Todos los sistemas mencionados deberán soportar un tipo de usuario que tenga privilegios especiales para acceso a los sistemas, para que esto le permita administrar la seguridad y realizar las tareas de soporte y administración.

- La asignación de privilegios de acceso a la información, deberá ser controlada mediante un proceso formal de autorización. Este proceso deberá:

  - Identificar los privilegios asociados con cada programa producto del sistema y el perfil al cual se deberá asignar.
  - Asignar privilegios únicamente a quien por sus funciones así lo requiera.

  - Estar basado en un proceso de autorización y registrar todos los privilegios asignados.

- Los privilegios serán asignados a grupos y nunca a usuarios específicos.

- La asignación de claves de acceso deberá ser controlada por un proceso de administración formal que:

  - Notifique de manera segura las claves iniciales de acceso a los usuarios.
  - Se debe evitar la notificación de claves de acceso a terceras partes. Los usuarios deben confirmar la recepción de claves de acceso.

- Todo usuario debe contar con una contraseña y ésta será normada de acuerdo a cada plataforma.

Acceso único a todas las plataformas

- Para mantener un control efectivo en el acceso a la información y a los servicios, El Departamento de Seguridad de Red, en coordinación con los dueños de información, deberá realizar en forma periódica, un proceso formal de revisión de los derechos de acceso de los usuarios.

- Con el fin de asegurar que los usuarios conectados a los servicios de cómputo no comprometan la seguridad de cualquier otro servicio, es necesario establecer un estricto control de acceso sobre toda conexión, autenticando usuarios y terminales.

- Un empleado no tendrá más de un user-ID para acceder a un sistema.

- Las contraseñas nunca se deberán comunicar a través de una línea telefónica de voz. Si una contraseña es revelada deberá ser modificada inmediatamente.

- Todos los componentes de infraestructura de red que tengan la posibilidad de acceso a través de control de contraseñas deberán ser estandarizados en cuanto a su sintaxis o conformación de la contraseña.

- La contraseña seleccionada deberá cumplir con las siguientes reglas:

    - Debe ser de al menos 8 posiciones de longitud.
    - Deberá contener al menos un caracter alfabético y uno no alfabético.
    - No deberá contener el Nombre de Usuario.
    - Al ser cambiado, éste no deberá ser igual que el inmediato anterior.

- Las contraseñas, llaves de encripción e información similar son confidenciales y no deben ser comunicadas ni compartidas.

NOTA: Para evitar comprometer los componentes de la infraestructura de red, queda estrictamente prohibida la transmisión de contraseñas de usuario, contraseñas locales de equipos de red, así como información confidencial de la empresa a través de sistemas de mensajería instantánea como lo es ICQ, MSN Messenger, o bien, por vía telefónica.

- Los servicios de red y de cómputo que puedan ser accedidos por un usuario o terminal en particular, deberán ser consistentes con las políticas de control de acceso.

- Los grupos lógicos de componentes de la infraestructura de red, por ejemplo ruteadores dentro del site, que tengan la misma lista de acceso pueden tener la misma contraseña, la cual pudiera ser compartida por el personal de soporte.

NOTA: No se deben asignar contraseñas idénticas a grupos de componentes de la infraestructura de red tan grandes que la infraestructura entera pueda ser comprometida en el caso de que una sola contraseña haya sido comprometida.

Recomendación para la selección de contraseñas

Una técnica que puede solucionar este problema consiste en seleccionar aleatoriamente dos palabras cortas y conectarlas por medio de un signo de puntuación. Esta combinación da como resultado una secuencia casi aleatoria de caracteres difícilmente adivinable pero que se puede recordar sin problemas. A continuación se presentan algunos ejemplos de contraseñas que utilizan esta técnica:

Pepe&Dia
Marzo!Tito
Equipo!Contra

Otro método para seleccionar contraseñas es tomar una frase que se vaya a recordar fácilmente y utilizar la primera letra de cada palabra. El resultado es una secuencia aleatoria de caracteres que se podrá recordar fácilmente. Por ejemplo, la expresión "se acabó lo que se daba" se convierte en la contraseña salqsd.

Lo importante es memorizar la contraseña y nunca escribirla en ningún sitio. Si se cree que no se podrá recordar si no se escribe, entonces lo mejor es hacerlo en un mensaje que incluya más palabras. Por ejemplo, si la contraseña es Modem!en puede escribirse en un papel que diga "No olvidar recoger el Modem! en el taller de reparaciones" el cual parece un recordatorio que evitará que otras personas descubran su contraseña.

1.4 PROCEDIMIENTOS ACTUALES POR EL ÁREA DE SEGURIDAD PARA EL INVENTARIO DE EQUIPOS Y USUARIOS, Y EL SEGUIMIENTO DE INCIDENTES DE SEGURIDAD

Actualmente los procedimientos de inventarios de equipos y usuarios, así como el manejo de incidentes de seguridad, se realizan de forma manual, en archivos de texto o de Microsoft Excel, dejando lugar a posibles errores o retardos en la entrega de resultados y atención a requerimientos.

1.4.1 Proceso de manejo y tratamiento de reportes de incidentes de seguridad

Ante la demanda de recursos de la red, también existe el interés de algunos usuarios para tener acceso a equipos, los cuales solamente deberían otorgar acceso a personal autorizado, o bien, la utilización de estos mismos equipos para el envío de mensajes o anuncios que terminan siendo información basura para los destinatarios, y que provocan que todos estos recursos de red funcionen de manera inapropiada.

Se consideran incidentes de seguridad los siguientes:

- Accesos no permitidos a la red que dañen la integridad de la información y/o desempeño.
- Mensajes de correo que por su contenido sean ofensivos o de mal agrado.
- Intentos de acceso no autorizado a la red
- Intento de acceso no autorizado a través del puerto 514 de TCP.
- Saturación del ancho de banda por tráfico generado por violaciones de red.
- Rastreo de vulnerabilidades en equipos de la red.
- Envío de gran cantidad de Pings (ICMP) utilizando dirección fuente falsa.
- Intentos de acceso no permitidos por el Protocolo Simple de Administración de Redes.
- Envío de correo basura utilizando el puerto 25 abierto en un servidor de correo.
- Exceso de tráfico provocado por Virus.
- Escaneo de puertos al Servidor DNS.
- Transferencia de zonas de DNS no permitida.
- Negación de consulta a DNS por posible infección de virus.
- Dirección que presenta posible infección por un WORM.

El proceso tendrá las siguientes características:

- El levantamiento de cada reporte se realiza incluyéndolo en un archivo de Excel, así como gran parte de su seguimiento y cierre de caso. Los incidentes son almacenados en archivos mensuales.

- Se revisa la no duplicidad de los reportes, buscando en el archivo el posible levantamiento anterior de una dirección específica.

- La consulta del seguimiento de los distintos reportes, puede ser consultada realizando una búsqueda de acuerdo a la dirección origen y fecha.

- Las notificaciones y avisos se realizan manualmente vía correo electrónico, y para los casos necesarios vía telefónica.

- El proceso está orientado a incidentes provenientes de clientes corporativos, o usuarios internacionales, excluyendo totalmente a clientes de servicio conmutados, los cuales son canalizados manualmente al área correspondiente vía correo electrónico.

El procedimiento cuenta con los siguientes pasos para registrar y manejar los incidentes de seguridad en la red:

Levantamiento

Consiste en dar de alta la información clave del reporte del incidente de seguridad en el archivo de Excel, en un nuevo renglón, indicando con la mayor exactitud posible la información del reporte, de acuerdo a las columnas que deben irse llenando y que se describen a continuación.

- Dirección IP del equipo atacante o fuente del abuso de red, el cual viene incluido en el reporte de ataque Subgerencia de Seguridad de Red.

- Identificación del enlace que conecta el último ruteador propio (administrado por la empresa) con el equipo perteneciente al cliente que realiza el ataque. Tomar los datos de dirección IP y nombre del ruteador de Acceso (propio) y ruteador o equipo de conexión externa.

  Para realizar este paso, se deberá primeramente, acceder a cualquier router de la empresa que se tengan en los catálogos, para que, desde ese punto, se pueda ejecutar el comando:

  Router>Traceroute [ipaddress]

  Donde *ipaddress* es la dirección IP del equipo reportado como fuente del ataque. El resultado de la ejecución de este comando, puede llevar a la dirección IP buscada, o bien, se puede perder la respuesta de los ruteadores externos que llevan a dicha dirección.

- Cuando se tengan estos datos, se deberá investigar en el **Whois** (Quien es) de las entidades que tienen el registro de dominios y direcciones IP asignadas a cada área del planeta, como pueden ser NIC, ARIN, LACNIC, APNIC, etc, los datos de contacto para la organización dueña de la dirección IP.

- Nombre del cliente, que se obtiene de las entidades que tienen el registro de dominios y direcciones IP mencionadas en el punto anterior.

- Fecha y hora del ataque, la cual es tomada del reporte recibido en el reporte canalizado a la Subgerencia.

- Tipo de ataque del reporte recibido, en el que se especifica de qué se trata el ataque o abuso relacionado con la dirección IP. Éstos pueden ser mensajes de correo no solicitados, **scaneo** (rastreo) de puertos, Intrusiones a los equipos sin autorización, apertura de puertos, intrusión, etc.

- Contacto técnico de la organización responsable, el cual es consultado en la base de datos de las entidades mencionadas con anterioridad. Este contacto puede ser consultado también en la base de datos de clientes de la empresa en el caso de que el incidente provenga de alguno de ellos. Los datos a tomar son: nombre del contacto técnico, teléfono y dirección de correo electrónico.

Notas.

- Debido a que existen reincidencias de ataques, se realiza una búsqueda previa de la dirección IP atacante en las hojas de Excel generadas con anterioridad por el área de Seguridad de Red, con el fin de obtener la información ya mencionada.

- En el caso de que ya se cuente con la información, el único dato que debe de actualizarse es la fecha y hora del ataque, lo demás se guardará como una copia del renglón que ya fue dado de alta con anterioridad.

Notificaciones de recepción y seguimiento de reportes de incidentes

De acuerdo a una plantilla de correo, se enviará una notificación por correo al responsable de la dirección que realiza el incidente, mediante la inclusión de los datos de hora, fecha, IP fuente, y tipo de incidente presentado. Este mensaje de correo se envía de forma manual para cada uno de los incidentes que se presentan.

Interacción con el responsable

Una vez que el responsable de la IP recibe la notificación, se puede tener cierta interacción entre El Departamento de Seguridad de Red y el cliente, trabajando en conjunto para darle solución a las vulnerabilidades de sus equipos que permiten que sean blancos de **hackers** (usuarios atacantes).

Cada vez que se interactúa con el responsable del incidente, se capturan todos los avances que se tengan para resolver el ataque, en una columna llamada "Comentarios" al final de cada registro del archivo de Excel.

Cierre

Una vez que el área reciba por parte del cliente la notificación de que el problema de vulnerabilidades en el o los equipos de su responsabilidad han sido resueltas, se procede a cerrar el reporte. Para cerrar el reporte, se marca con un color diferente al predeterminado el o los renglones contenidos en el archivo de Excel que involucran al caso presentado.

1.4.2 Inventario de equipos de red que constituyen la infraestructura de la empresa

El inventario de los equipos que se encuentran en operación en la red, y los cuales pueden ser ruteadores, servidores de acceso, LAN switches, etc., se tienen almacenados en varios archivos de texto de acuerdo al tipo de servicio que proporcionan y con un formato determinado, el cual consta del nombre del equipo dentro de la red, así como su dirección IP, ambos datos separados por dos puntos (:). Por ejemplo:

rtr-villacoapa-1.mexnet.com.mx:192.168.0.1:
rtr-villacoapa-2. mexnet.com.mx:192.168.0.2:

Teniendo entonces, un archivo que incluye todos los LAN switches, otro archivo con la información de los servidores de acceso, y así sucesivamente.

Para los equipos de red que requieren la configuración de una contraseña para obtener acceso a ellos, ésta o éstas se incluyen en un campo más, de igual forma separada por dos puntos. Por ejemplo:

nas-villacoapa-1. mexnet.com.mx:192.168.0.3:abcd1234:
nas-villacoapa-1. mexnet.com.mx:192.168.0.4:efgh5678:

En el ejemplo anterior se tiene que el nombre del equipo es nas-villacoapa-1. mexnet.com.mx, la dirección IP que le pertenece es 192.168.0.3 y la contraseña de acceso es abcd1234.

Actualmente en estos archivos, no se lleva un control de la fecha de alta de un nuevo equipo, simplemente se agrega o se elimina dependiendo de los movimientos que se presenten en la red.

1.4.3 Inventario de usuarios que tienen acceso a la infraestructura de red

El inventario de los usuarios autorizados para intervenir las diversas plataformas de equipos de red en la empresa se lleva mediante un archivo de Excel, en el cual se separa por grupos o perfiles de usuarios, así como los privilegios de acceso que se aplican al perfil de acuerdo al área dentro de la organización y las funciones que realizan.

Las plataformas existentes en los equipos de red, depende de la manera de acceder a ellos, y los grupos de usuarios que tendrán dicho acceso. Así, por ejemplo, para los equipos que requieren de un servidor de autenticación para validar que un usuario tenga o no permiso para entrar a ellos mediante un protocolo de autenticación determinado, por ejemplo **TACACS+**[1] (Terminal Access Controller Access Control System – Sistema de Control de Acceso a Terminales) o **RADIUS**[2] (Remote Authentication Dial In User Service – Servicio de Autenticación de Usuarios Remotos

[1] Es un protocolo que delega la información de usuario y contraseña a un servidor centralizado, el cual provee los servicios de autenticación (credenciales de acceso de cada usuario), autorización (qué puede hacer) y contabilización (bitácora de qué está haciendo) de cuentas de usuarios.
[2] El servicio RADIUS se emplea para la autenticación, autorización y cuentas de usuarios remotos que traten con el protocolo RADIUS. Este protocolo es el encargado de la validación y asignación de cuentas de los usuarios que acceden a Internet mediante acceso telefónico.

por Acceso Telefónico), se tiene un registro de todos los usuarios y grupos con sus respectivos privilegios de acceso, los cuales se refieren a los comandos de configuración que podrán utilizar en los equipos dependiendo de su función.

Así por ejemplo para el acceso a los equipos que requieren validación por TACACS+ se tiene un archivo con los perfiles, usuarios y permisos, organizados de acuerdo al formato que se muestra en las figuras 1.4.3.1 y 1.4.3.2 en un archivo de Microsoft Excel.

Departamento: Fallas **Grupo: I-FAL**	**Departamento: Configuraciones** **Grupo: I-CFG**
Alejandro Garrido Sánchez	Miguel Salinas
Adrián Paxtian Ávila	José Luis Leonardo López
Arely Berenice Ojeda Padilla	
Edgar Fernando Sánchez Clorio	
Adriana Esther Cruz Avendaño	
José Antonio Hernández Cruz	
Juan Carlos Solís Crespo	
Luis Alfredo González García	

Figura 1.4.3.1 Organización de perfiles y usuarios

Departamento: Fallas **Grupo: I-FAL**	**Departamento: Configuraciones** **I-CFG**
permit configure terminal	deny router bgp
permit interface	deny router ospf
permit ip	deny router eigrp
permit controller	deny no router bgp
permit terminal	deny no router eigrp
permit clear	deny no router ospf
permit show	deny debug
permit bandwidth	
permit clock	
deny erase	
deny write erase	

Figura 1.4.3.2 Organización de perfiles y permisos

1.4.4 Notificaciones

Las notificaciones derivadas de los incidentes de seguridad, las notificaciones de información de activación de cuentas de usuarios personalizados a sus responsables y las notificaciones de seguridad difundidas por el Departamento de Seguridad de Red hacia las diferentes áreas de la empresa, se realizan de manera manual, utilizando una aplicación cliente de correo electrónico como Microsoft Outlook o Microsoft Outlook Express, incluyendo la información necesaria para cada caso.

Para las notificaciones de incidentes de seguridad se consideran las siguientes.

- Notificación a responsables de IPs que presentan incidentes, que se está haciendo uso indebido de los recursos de su red, indicando la dirección IP fuente, la fecha, la hora y el tipo de incidente de que se trata.

Para las notificaciones de cuentas de usuario se incluye:

- Nombre de usuario
- Contraseña de acceso
- Contraseña de acceso a nivel privilegiado en las plataformas en las que aplica
- Advertencia de uso adecuado de la información enviada.

Las notificaciones de seguridad son, por ejemplo:

- Envío de boletines de seguridad publicadas por entidades mundiales de seguridad.
- Envío de descripciones de vulnerabilidades que se presenten en sistemas operativos conocidos, como por ejemplo la plataforma Windows.
- Envío de información de aparición de nuevos virus o gusanos que afecten la operación de los equipos o servidores que se encuentren en la red.

CAPÍTULO II
TEORÍA BÁSICA

2.1 BASES DE DATOS RELACIONALES

Introducción

La base de datos relacional es un modelo de datos en el cual no existe una jerarquía entre los campos de datos de un registro, por lo que cada campo puede ser usado como un identificador o llave. Los datos son almacenados como una colección de valores en forma de simples registros llamados tuplas ("tuples") o duplas.

Cada tupla representa en realidad un conjunto de valores relacionados permanentemente. Estas tuplas son agrupadas en tablas bidimensionales, donde cada tabla generalmente es almacenada como un archivo separado, incluso los resultados de cualquier consulta son otra tabla. La tabla en sí representa las relaciones entre todos los atributos que ella contiene y en consecuencia es llamada una relación.

En cada tabla, las filas y las columnas, en principio, carecen de orden, es decir, el orden en el que se muestren las filas y las columnas no importa. Las filas sólo se ordenan si se le indica a la base de datos que lo haga, mediante el correspondiente comando, de no ser así, el orden será arbitrario, y puede cambiar en caso de tratarse de una base datos dinámica. El orden de las columnas lo determina cada consulta.

Modelización de datos

Un modelo es la representación simplificada de la parte que nos interesa del sistema. El modelo es aceptable si el resultado de una operación sobre el modelo es considerado como equivalente al resultado de la operación correspondiente efectuada en el sistema real.

La modelización es el proceso sistemático y racional conducente a la creación de un modelo adaptado a un objetivo particular, de tal manera que se convierta en el medio de comunicación entre quienes participan en el proyecto para comprender el conjunto

de los datos y sus relaciones con los cuales cada usuario trabajará. El modelo facilitará la actualización y evolución del sistema en el momento que se requiera ya que permitirá reanalizar fácilmente los datos con los que trabaja la organización. La modelización se ejemplifica en la figura 2.1.1

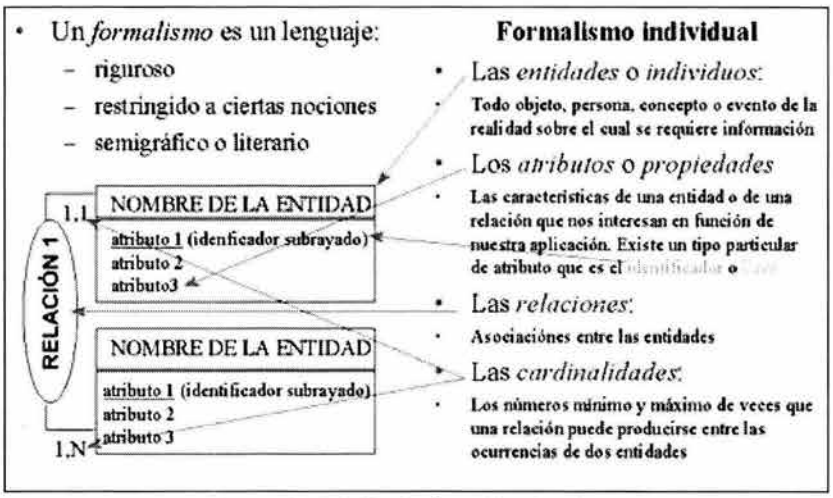


Figura 2.1.1 Modelización de datos

Diseño de las bases de datos relacionales

Cada tabla tiene una clave primaria, un identificador único, compuesto por una o más columnas. La mayoría de las claves primarias están formadas por una única columna (atributo).

Para establecer una relación entre dos tablas es necesario incluir, en forma de columna, en una de ellas la clave primaria de la otra. A esta columna se le llama clave secundaria.

Estos dos conceptos --clave primaria y secundaria-- son los más importantes en el diseño de bases de datos. Es importante dedicarles tiempo, para entender bien en qué consisten y cómo funcionan.

Las cualidades de un buen diseño de base de datos involucran:

- Reflejar la estructura del problema en el mundo real.
- Ser capaz de representar todos los datos esperados, incluso con el paso del tiempo.
- Evitar el almacenamiento de información redundante.
- Proporcionar un acceso eficaz a los datos.
- Mantener la integridad de los datos a lo largo del tiempo.
- Ser claro, coherente y de fácil comprensión.

En el entorno actual de desarrollo de sistemas, la base de datos relacional es el método más usado para el almacenamiento de datos. Algunos diagramas para modelar aspectos del diseño de bases de datos relacionales no cubren toda la semántica involucrada en el modelado relacional, mayoritariamente la noción de atributos clave que relacionan entre sí las tablas unas con otras.

Para capturar esta información, se recomienda un Diagrama Entidad-Relación (ER diagram), el cual será la muestra de una versión simplificada y representa los datos mediante una serie de entidades (una clase de objetos o conceptos claramente identificable) que disponen de atributos. Las entidades establecen interrelaciones con otras entidades.

Las relaciones de herencia son referenciadas directamente a super-sub relaciones entre entidades en el diagrama de relación de entidad. Las relaciones super-sub entre entidades se resuelven por las estructuras de tablas actuales.

Ya en el Diagrama de Entidad-Relación, es posible empezar el proceso de determinar cómo el modelo relacional encaja; y qué atributos son claves primarias, claves secundarias, y claves externas basadas en relaciones con otras entidades.

El resultado de este proceso es una base de datos normalizada que facilita el acceso a los datos y evita su duplicado. El diseño formal de una base de datos se centra en la normalización de la base y en asegurar que el diseño se ajuste a un nivel de normalización. La idea es construir un modelo lógico que sea conforme a las reglas de normalización de datos. La aplicación de una de estas reglas es una operación que toma una relación como argumento de entrada y da como resultado dos o más relaciones que cumplen lo siguiente:

- La relación a la que se le aplica la regla, es desestimada en el nuevo esquema relacional.
- No se introducen nuevos atributos en el esquema relacional que resulta de la normalización.
- Los atributos de la relación a la que se le aplica la regla de normalización, pasan a formar parte de una o más de las relaciones resultantes.

Existen varias reglas de normalización, sin embargo, por lo general, es suficiente garantizar que se cumplen las tres primeras formas normales, las cuales se enuncian a continuación:

Primera Forma Normal (FN1).- Una relación R satisface la primera forma normal (FN1) si cumple las condiciones de una relación que se indican enseguida:

- En las celdas de la tabla bidimensional debe haber valores individuales; no se aceptan arreglos como valores.

- Todas las entradas en cualquier columna deben ser del mismo tipo. Por ejemplo, si una columna contiene números, cada renglón en esa columna debe contener sólo números.

- Cada columna debe tener un nombre único y no importa el orden de las columnas en la tabla.

- No puede haber dos renglones idénticos.

Segunda forma normal (FN2).- Una relación R satisface la segunda forma normal (FN2) si, y solo si, satisface la primera forma normal y cada atributo de la relación depende funcionalmente de forma completa de la clave primaria de esa relación. En otras palabras, cualquier relación cumple la FN2 si todos sus atributos no-llave son dependientes en todo del atributo llave.

Tercera forma normal (FN3) .- Una relación está en la tercera forma normal si está en la segunda forma normal y no tiene dependencias transitivas.

Para diseñar el Diagrama Entidad-Relación, el proceso es:

- Identificar las entidades que debe presentar la base de datos.

- Determinar las cardinalidades de las interrelaciones establecidas entre las distintas entidades y clasificar estas interrelaciones entre los siguientes tipos:

    - Uno a uno (p. ej., un host sólo tiene una dirección).
    - Uno a muchos (p. ej., en un host pueden ocurrir varios incidentes).
    - Muchos a muchos (p. ej., un host lo pueden acceder varios usuarios y cada usuario puede acceder varios hosts).

- Dibujar el Diagrama Entidad-Relación.

- Determinar los atributos de cada entidad.

- Definir la clave primaria (única) de cada entidad.

Para pasar del Diagrama Entidad-Relación al diseño de la base de datos, el procedimiento es:

- Las entidades entre las que hay una interrelación uno a uno se deben fusionar en una sola entidad.

- Cada una de las entidades que quedan se convierte en una tabla con una clave primaria y una serie de atributos, de los cuales algunos pueden ser claves secundarias.

- Las interrelaciones uno a muchos se transforman en atributo y clave secundaria de la tabla que representa a la entidad situada del lado de la interrelación correspondiente a muchos.

- Las interrelaciones muchos a muchos entre dos entidades pasan a ser una tercera tabla con claves secundarias procedentes de ambas entidades. Estas claves secundarias deberán formar parte de la clave primaria de la tabla en la que se convierte la interrelación, cuando corresponda.

Hay una serie de herramientas disponibles en el mercado que pueden automatizar el proceso de conversión de un Diagrama Entidad-Relación en un esquema de base de datos.

2.2 MICROSOFT SQL SERVER 2000, CARACTERÍSTICAS, VENTAJAS Y DESVENTAJAS

Pantalla principal del SQL Server Enterprise Manager

A continuación se muestra en la figura 2.2.1 la pantalla principal del SQL, a través de la cual se ejecutan las funcionalidades del SQL.

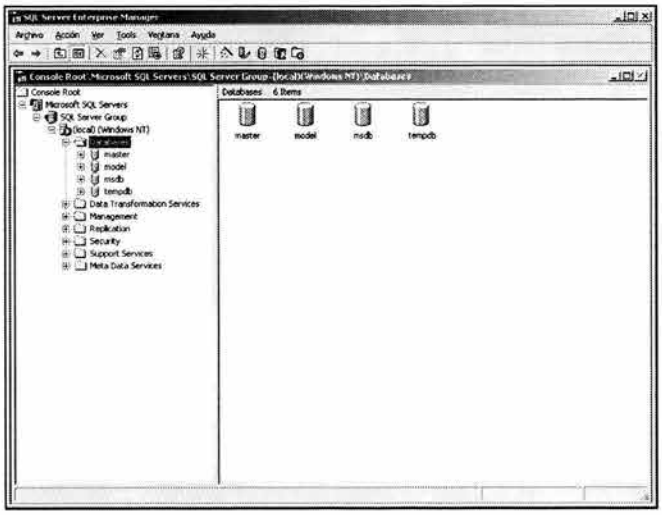


Figura 2.2.1 Pantalla principal de SQL Server Enterprise Manager.

Ventajas del cliente

- Facilidad de uso.
- Manejo de múltiples plataformas de hardware.
- Manejo de múltiples aplicaciones de software.
- Familiar al usuario.

Ventajas del servidor

- Confiable.
- Tolerante a fallas.
- Hardware de alto desempeño.
- Expone los datos como servicios en la web.

Portabilidad

Las bases de datos pueden desarrollarse fácilmente ya sea en una red de microcomputadoras y operarse en un equipo mainframe o una mini computadora, sin importar su sistema operativo. Cuenta con soporte de **SAN** (Storage Area Network - Red de Área de Almacenamiento), lo que permite una mayor comunicación entre servidores.

Compatibilidad

- Los **DBMS** (Database Management System – Sistema de Administración de Base de Datos) se pueden ejecutar ya sea en computadoras personales, microcomputadoras, mainframes y computadoras con procesamiento paralelo masivo, así como en distintas arquitecturas de hardware y software sin tener la necesidad de cambiar una sola línea de código. El optimizador de consultas soporta paralelismo entre las mismas lo que implica la capacidad de procesar una sola consulta en múltiples CPU.

- Primera base de datos que ofrece una compatibilidad de código del 100%.

- Primera base de datos con **DTS** (Data Transformation Service - Servicios de transformación de datos integrados). Con DTS se pueden importar y exportar datos entre varias fuentes de datos heterogéneas y destinos de datos, es decir, transferir y transformar los datos automáticamente.

Conectividad

- Los DBMS pueden trabajar con información almacenada con otros sistemas de bases de datos, así como también almacenar los datos y acceder a ellos desde otros paquetes de software.

- Es la primera base de datos que ofrece la administración multiservidor para un gran número de servidores.

- Acceso universal a los datos (Universal Data Access), la estrategia de Microsoft para permitir el acceso de alto rendimiento a una gran cantidad de fuentes de información.

- Se puede utilizar varios CPU al insertar, seleccionar, actualizar y eliminar.

- La estrategia de Microsoft afirma que SQL Server es la base de datos que lleva a cabo la creación, administración y distribución de las aplicaciones empresariales en forma más sencilla, esto significa proporcionar a los desarrolladores un modelo de programación simple y rápido, eliminar la necesidad de administrar la base de datos en las operaciones habituales y proporcionar herramientas sofisticadas, para realizar las operaciones más complejas en distintos servidores.

- Permite ejecutar varias aplicaciones de forma fiable con instancias separadas de base de datos por cliente o aplicación.

- La capacidad para operar con otros productos incluye soporte para una conectividad sin problemas entre sistemas y fuentes de datos.

Seguridad

- Verificaciones de usuarios, mantener clientes diferentes en una misma base de datos y señalar ciertos datos que solo podrán acceder determinados usuarios así como la codificación de información privada.

- El administrador puede programar permisos por tabla, columna o fila.

- El acceso a los datos es por medio de credenciales de seguridad formal.

- Por medio del sistema operativo se permite la restricción de los movimientos que pudieran hacerse con los archivos, así como controlar los accesos con cuentas. A esto se le conoce como autenticación.

- La seguridad comprende protección y codificación de tablas de datos, columnas y filas, así como las transferencias de datos entre un cliente y un servidor como auditorias que identifican violaciones a la seguridad.

Administración

- Funcionalidades de administración y optimización de la memoria, del CPU y de disco, de manera que se reduce el tiempo para la administración.

- Primera base de datos que soporta la configuración automática y la auto-optimización por medio del servicio Agente SQL Server.

- Comprende la interacción que se requiere para el desempeño óptimo de la base de datos, las tareas que incluyen instalación y configuración, mantenimiento y supervisión de recursos.

Rendimiento

Permiten una alta disponibilidad de aplicaciones sin necesidad de una reconfiguración de datos.

Herramientas de desarrollo

- Funcionan con un amplio conjunto de herramientas de desarrollo, herramientas de consulta para el usuario final, aplicaciones comerciales y herramientas de gestión de la información del ámbito corporativo.

- Diseño de soluciones económicas de almacenamiento de datos mediante la combinación de tecnologías, servicios y alianzas entre fabricantes (Microsoft Alliance for Data Warehousing). Entre estas innovaciones se incluyen:

    - Generación de informes y análisis corporativos hasta el modelado de datos y el soporte de la toma de decisiones.
    - Generación de Microsoft Repository (Deposito de Micrososft), una infraestructura común para compartir la información.

Requerimientos del Sistema

Microsoft SQL Server 2000 opera en computadoras con procesador Intel o compatibles Pentium, Pentium Pro, Pentium II o superiores. Éstos deben tener como mínimo 166MHz. Las ediciones y versiones de SQL Server 2000 necesitan la siguiente memoria RAM:

- Enterprise Edition: 64 MB de mínimo ó 128 MB recomendado.
- Standard Edition: 64 MB de mínimo.
- Personal Edition: 64 MB en Windows 2000, 32 MB en todos los demás sistemas operativos.

- Developer Edition: 64 MB de mínimo
- Desktop Engine: 64 MB mínimo en Windows 2000, 32 MB en los demás sistemas operativos

SQL Server 2000 debe tener los siguientes requerimientos dependiendo de los componentes de instalación seleccionados:

- Database components: 95 a 270 MB, 250 MB típica.
- Analysis Services: 50 MB mínimo, 130 MB típica.
- English Query : 80 MB.
- Desktop Engine only:44 MB.
- Monitor con resolución VGA; las herramientas de gráficos de SQL Server requieren un monitor con resolución 800x600 ó superior.
- CD-ROM y un ratón Microsoft o compatible.
- Internet Explorer 5.0 ó posterior y es soportado por los siguientes sistemas operativos:
    - Windows 2000
    - Microsoft Windows NT version 4.0 Service Pack 5 ó posterior
    - Windows Millennium Edition
    - Windows 98
    - Windows 95

2.3 VISUAL BASIC 6.0, CARACTERÍSTICAS, VENTAJAS Y DESVENTAJAS

Introducción

Visual Basic es actualmente el lenguaje de programación más popular del mundo. Se trata de un producto con una interfaz gráfica de usuario que sirve para crear aplicaciones para Windows basado en el lenguaje **Basic** (Beginners All-Purpose Symbolic Instruction Code) y la programación orientada a objetos.

La palabra "Visual" hace referencia al método que se utiliza para crear la interfaz gráfica de usuario. En lugar de escribir numerosas líneas de código para implementar una interfaz, se utiliza el ratón para arrastrar y colocar los objetos prefabricados al lugar deseado dentro de un formato.

La palabra "Basic" hace referencia al lenguaje Basic, un lenguaje utilizado por más programadores que ningún otro en la historia de la informática. Visual Basic ha evolucionado a partir del lenguaje Basic original y ahora con centenares de instrucciones, funciones y palabras clave, muchas de las cuales están directamente relacionadas con la interfaz gráfica de Windows.

Visual Basic permite crear programas para uso personal, para un grupo de trabajo, para una empresa, aplicaciones distribuidas a través de Internet, aplicaciones de bases de datos y otras muchas que se puedan imaginar.

Para crear una aplicación, se crean ventanas y sobre ellas se dibujan controles (etiquetas, botones, cajas de texto, etc.) y a continuación se escribe el código fuente relacionado con cada objeto. Esto es, cada objeto está ligado a un código que permanece inactivo hasta que se dé el evento que lo activa (por ejemplo, un clic del ratón).

Visual Basic proporciona herramientas que permiten crear ventanas y controles sin escribir código. También incluye un entrono de desarrollo que permite ejecutar todas las tareas de edición, ejecución y mantenimiento de programas de una forma fácil y cómoda. Así mismo, pone a disposición del usuario una ayuda en línea completa, lo que permitirá solucionar cualquier duda que surja mientras se crea una aplicación. Todo esto hace posible que en muy poco tiempo se puedan escribir programas simples y potentes.

Características de Visual Basic

Visual Basic incluye como características más sobresalientes las siguientes:

- Una biblioteca de clases que da soporte a los objetos Windows tales como ventanas, cajas de diálogo, controles (por ejemplo, etiquetas, cajas de texto, botones de pulsación, etc.)

- Un control que permite utilizar las cajas de diálogo más comúnmente utilizadas (abrir, guardar como, imprimir, color y fuentes).

- Un entorno de desarrollo integrado, figura 2.3.1, (editor de texto, intérprete, depurador, examinador de objetos, explorador de proyectos, compilador, etc.). Visual Basic fue diseñado para ser un intérprete, lo que favorece la creación y la depuración de una aplicación, y a partir de la versión 5 incluyó también un compilador que permite generar archivos .exe favoreciendo así la ejecución.

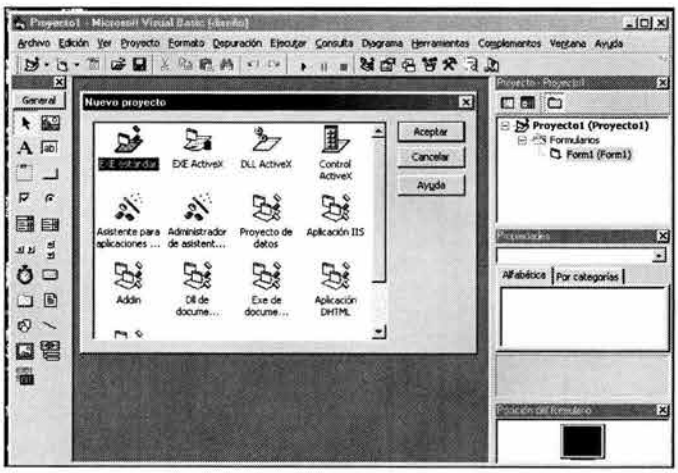


Figura 2.3.1 Entorno de desarrollo de Visual Basic

- El editor de textos le ayuda ahora a completar cada una de las sentencias visualizando la sintaxis correspondiente a las mismas.

- Galería de objetos incrustados y vinculados OLE (Object Linking and Embedding). Esto es, software autocontenido en pequeñas y potentes unidades o componentes de software para reutilizar en cualquier aplicación.

- Asistentes para el desarrollo de aplicaciones como se muestra en la figura 2.3.2, barras de herramientas, formularios de datos, empaquetado y distribución, creación de la interfaz pública de controles ActiveX, páginas de propiedades, objetos de datos y generador de clases.

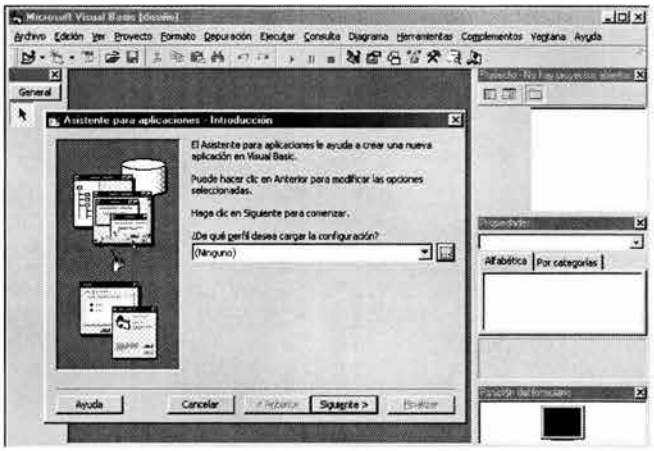


Figura 2.3.2 Asistentes de Visual Basic.

- Visualizaciones y manipulación de datos de otras aplicaciones Windows utilizando controles OLE.

- Una interfaz para múltiples documentos MDI (Múltiple Document Interface) que permite crear una aplicación con una ventana principal y múltiples ventanas de documento. Un ejemplo de este tipo de aplicaciones es Microsoft Word.

- Editar y continuar. Durante una sesión de depuración, se pueden realizar modificaciones en el código de la aplicación sin tener que salir de dicha sesión.

- Creación y utilización de bibliotecas dinámicas DLL (Dynamic Link Libraries).

- Soporte para la programación de aplicaciones para Internet; forma parte de este soporte la tecnología de componentes activos (ActiveX).

- Soporte para el estándar COM (Component Object Model - Modelo de objeto componente) en otras palabras, componente de software al que pertenecen los componentes activos (ActiveX o formalmente controles OLE).

- Acceso a bases de datos a través del control de datos ADO, utilizando el motor de Access o controladores ODBC.

- Acceso a bases de datos utilizando OLE DB como un proveedor de datos y objetos ADO (ActiveX Data Object – Objetos ActiveX para acceso a datos), como tecnología de acceso a datos, para satisfacer los nuevos escenarios demandados por las empresas, tales como los sistemas de información basados en la WEB.

- Biblioteca para SQL que permite manipular bases de datos relacionales, tales como Microsoft Access (SQL-Structured Query Language) .

- Un administrador visual de datos para manipular bases de datos.

- Un programa para añadir ayuda en línea; esta herramienta permite la creación de archivos de ayuda estilo Windows (hcw.exe – Help Workshop).

Cuando se combinan estas características, algunas de ellas sólo disponibles en la versión profesional y empresarial, se dispone de un sistema de desarrollo que permite diseñar rápidamente aplicaciones sofisticadas.

Instalación de Visual Basic

Existen tres ediciones de Visual Basic; la estándar o de aprendizaje, la profesional y la empresarial. La edición estándar permite crear robustas aplicaciones para Microsoft Windows; incluye todos los controles intrínsecos, los controles rejilla, cuadro de diálogo estándar y los controles enlazados a datos, además de los controles fichas etiquetadas, barras de herramientas, barra de estado, barra de progreso, vista en forma de árbol, vista en forma de lista, lista de imágenes, control deslizante y lista desplegable de imágenes. También incluye una versión compilada del administrador visual de bases de datos (VisData). La edición profesional incluye todas las características de la edición estándar, así como controles ActiveX adicionales, el diseñador de aplicaciones para Internet Information Server, el diseñador de páginas HTML dinámicas y el código fuente del administrador visual de bases de datos. La edición empresarial incluye todas las características de la edición profesional, así como herramientas de Back Office como SQL Server, Microsoft Transaction Server, Internet Information Server, Visual SourceSafe, etc.

Requerimientos Mínimos

Para instalar Visual Basic se debe verificar que la computadora cumple con los requerimientos que se indican a continuación:

- Microprocesador Pentium 90 MHz o superior.
- Disco duro con espacio disponible de 80 MB para poder realizar una instalación completa de la edición estándar.
- Unidad de CD-ROM.
- Ratón.
- Tarjeta de video soportada por Windows.
- 32 MB de memoria o más.
- Microsoft Windows 95 ó posterior, o Windows NT 3.51 ó posterior.
- Microsoft Internet Explorer versión 4.01 ó posterior.

Si el sistema cumple con los requerimientos mínimos, se puede comenzar a instalar Visual Basic.

Ventajas y desventajas de Visual Basic

Visual Basic es un producto que sirve para crear aplicaciones para Windows basado en el lenguaje Basic y en la programación orientada a objetos con una interfaz gráfica de usuario que lo hace muy fácil de manejar.

Visual Basic incluye un entorno de desarrollo que permite realizar todas las tareas de edición, ejecución y mantenimiento de programas de una forma fácil y cómoda. También proporciona asistentes que facilitan crear aplicaciones genéricas, de acceso a bases de datos, para Internet, así como para añadir un sistema de ayuda en la aplicación, o bien generar un medio para distribuir la aplicación.

2.4 HTML y ASP, características, ventajas y desventajas

HTML

Se puede describir a **HTML** (Hyper-Text Markup Protocol) como un conjunto de códigos especiales llamados **tags** (etiquetas), las cuales le indican al **web browser** (navegador web) como mostrar un documento de hipertexto. Es una colección de estilos que definen varios componentes de la página web que se está desplegando. Estas páginas son transferidas entre los servidores de **WWW** (World Wide Web – Red Mundial) y los navegadores de los clientes mediante el protocolo **HTTP** (Hypertext Transfer Protocol-Protocolo de Transferencia de Hipertexto)

Todos los documentos en HTML se escriben en formato de texto plano, haciendo que éste pueda ser leído universalmente por cualquier navegador web existente y en diferente tipo de plataforma de cómputo.

Un archivo HTML tiene generalmente la extensión .html o .htm. En general los tags son utilizados para identificar la estructura del documento así como las ligas de acceso a otras páginas. Las capacidades y características de cada navegador de web determinan la apariencia que tendrá el documento en la pantalla.

En un documento HTML, se incluyen elementos como:

- El título del documento.
- Párrafos
- Listas ordenadas, numeradas y anidadas.
- Puntos de inserción para gráficos o imágenes.
- Énfasis especial en cierto texto y frases.
- Áreas con formato especial en el documento.
- Ligas, que dirigen el contenido del navegador a otra página web.
- Tablas.
- Formas.

El elemento básico de HTML es el párrafo. El navegador lee y escribe en pantalla todo el contenido del párrafo de izquierda a derecha y de arriba hacia abajo, ajustando cualquier texto que no quepa en una sola línea y posicionándolo en la línea siguiente.

El HTML es un lenguaje de interpretación, el navegador crea una página web a partir del código fuente que recibe, y lo interpreta para mostrar la página que se ve en pantalla. En otras palabras, el navegador despliega la página a partir de las instrucciones escritas en HTML, y debido a esto es que diferentes navegadores pueden mostrar la misma página web de manera diferente.

La desventaja principal de un documento creado a partir de código HTML es que genera páginas estáticas, en el sentido de que, a efectos de usuario, el único proceso realizado es el de visualización de contenidos por parte del navegador del cliente.

En el momento en que se requiere una interacción mayor entre los usuarios y el sistema que soporta las páginas web, surge la necesidad de reunir y procesar las peticiones del cliente con el fin de ofrecerle información mejor dirigida y elaborada. Lo anterior crea la necesidad de dotar a alguna fase de procesamiento al intercambio de información entre los usuarios y el servidor de páginas web, por lo que se introduce el concepto de **ASP** (Active Server Pages – Páginas Activas en el Servidor) y **CGI** (Common Gateway Interface – Interfase de Entrada Común).

Así, la utilización de HTML sigue resultando conveniente, en combinación con ASP y CGI, debido a que forman la base necesaria para la presentación de datos en muchos tipos de situaciones, influyendo también la sencillez con que se pueden crear, instalar y mantener.

ASP

La tecnología ASP ha sido desarrollada por Microsoft para facilitar la creación de sitios web, ya que una página ASP puede ser diseñada con editores HTML y puesto que las instrucciones ejecutables y el código HTML están suficientemente delimitados. Así mismo pueden utilizarse diversos lenguajes para la programación de la funcionalidad de las páginas activas. Entre estos lenguajes se encuentran Visual Basic Script y Java Script. Los desarrollos en ASP no necesitan ningún procedimiento de compilación que retarde el proceso de petición y descarga de páginas web, y los errores de programación no provocan la caída del servidor web.

Desde ASP se pueden realizar accesos a componentes que se ejecutan en el servidor, de esta manera, por ejemplo, se hace un uso simple de controles ODBC (Open DataBase Connectivity – Conectividad a Bases de Datos Abiertas) para el acceso a distintos tipos de bases de datos.

Las páginas web que devuelve el servidor tras la ejecución de las instrucciones, están formadas por secuencias HTML visualizables en cualquier navegador.

ASP proporciona un método eficiente y sencillo de crear sitios web con páginas dinámicas y acceso a base de datos. Para que un usuario realice una petición de página web, deberá proporcionar en su navegador una dirección que indique un archivo con extensión .asp.

Cuando se trabaja con **IIS** (Internet Information Server – Servidor de Información de Internet) y ASP, el servidor analiza las peticiones de la página que recibe. Si se encuentra con una solicitud de página con extensión .asp en lugar de .htm o .html, entonces se apoya en la aplicación (archivos DLL de Windows) instalada en el servidor que sirve de soporte para la ejecución de las páginas ASP.

Esta aplicación diferencia las líneas HTML de las instrucciones que dan funcionalidad a las páginas activas. Cuando se determina el lenguaje en el que se encuentran los **scripts** (programas) da paso al motor de ejecución de scripts adecuado, realizando el análisis sintáctico y ejecución de las instrucciones. Los motores de ejecución de los scripts se encuentran, con llamadas a componentes externos con los que deben interactuar, tales como componentes de conexión a bases de datos. Posteriormente, el usuario recibe como respuesta el contenido de un archivo HTML que se ha formado uniendo las instrucciones HTML originales de la página ASP con las instrucciones que se han generado tras la ejecución de los scripts. La figura 2.4.1, muestra el mecanismo de obtención de una página de respuesta con ASP.

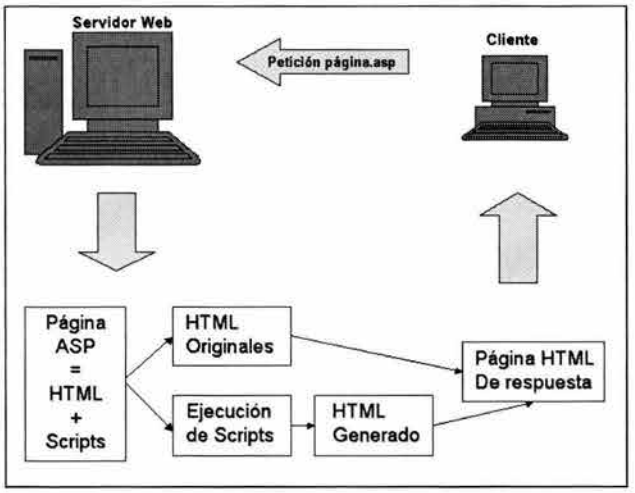


Figura 2.4.1 Obtención de una página de respuesta con ASP

Existen diferentes ventajas que nos otorga el uso de páginas dinámicas utilizando la tecnología ASP:

- Manejo de información centralizada. Todos los datos permanecen en un lugar central, el cual es el servidor.

- Los procesos se ejecutan en el servidor y por razones de seguridad no se transfieren a los clientes.

- Se asegura que todos los clientes puedan ver correctamente las páginas web, independientemente del tipo y versión de su navegador y del equipo que posean. Las páginas activas en el cliente se basan actualmente en tecnologías muy dependientes del explorador y la plataforma del usuario. Por ejemplo, un navegador Netscape no ejecutaría instrucciones en Visual Basic Script.

- En el caso en que los usuarios contaran con la plataforma y navegador adecuados, no siempre están dispuestos a descargar componentes ejecutables en sus equipos.

- Cuando el tamaño del programa es grande, y el tiempo de ejecución corto, puede resultar más rentable transferir los resultados obtenidos una vez ejecutado el programa en el servidor, en lugar de enviar el programa al cliente.

- La facilidad de acceso a bases de datos utilizando el componente ADO (ActiveX[3] Data Objects – Objetos de Datos ActiveX). La sencillez de uso y la integración con otros productos de Microsoft.

- La cantidad de servidores basados en el sistema operativo Microsoft Windows y su servidor IIS, ha llevado a que esta tecnología sea muy demandada.

- La posibilidad de utilización de multitud de objetos integrados y no integrados.

- La eficiencia en la ejecución.

2.5 Sistema Operativo Windows 2000 Server y Windows XP

Windows 2000 Server

Windows 2000 es el sistema operativo sucesor de NT. Existen tres variantes: Windows 2000 Professional (profesional), Windows 2000 Server (Servidor) Y Windows 2000 Advanced Server (Servidor Avanzado). La primer opción es para equipos que son

[3] La tecnología ActiveX de Microsoft permite la ejecución de código máquina (creado por los programadores de aplicaciones Web) en los equipos de los usuarios. Es decir, es posible vincular como objeto en una página web un programa que siga el estándar ActiveX y ejecutarlo en los equipos de los clientes que carguen la página. Esta tecnología permite distribuir con facilidad código a través de Internet.

utilizados y administrados directamente por el usuario final; debido a que son las versiones servidor las que nos interesan, no nos ocuparemos más de esta variante.

Windows 2000 Server, soporta hasta 4 procesadores, contiene funciones de servidor de impresión, servidor de archivos, de aplicaciones, de web y de FTP. Se utiliza en empresas de pequeñas a medianas.

Windows 2000 Advanced Server soporta hasta 8 procesadores y está pensado para funcionar como servidor departamental de aplicaciones en empresas medianas a grandes, con más de un dominio y tareas de misión crítica. Entre otras prestaciones, incluye soporte para RAID (Redundant Array of Independent Disks - Arreglo Redundante de Discos Independiente) y tolerancia a fallas.

Windows 2000 Data Center Server (Servidor Central de Datos) soporta hasta 32 procesadores y sólo se consigue sobre pedido. Está destinado a grandes empresas que requieran análisis econométricos[4], simulaciones científicas e ingenieriles a gran escala, etc.

Instalación de las Versiones Servidor de Windows 2000

La instalación de Windows 2000 versiones Server y Advanced Server requieren NT o una instalación limpia. El proceso empieza simplemente ejecutando el archivo Setup. Tras unos breves cuadros de opciones para la selección del lenguaje y de accesibilidad, se procede a la copia de archivos de instalación en el disco duro. Previamente, el asistente advertirá si uno desea convertir el sistema de archivos FAT o FAT32 a NTFS. Se recomienda hacerlo, ya que este sistema permite utilizar más eficientemente las funciones de administración de archivos. Una vez terminado, el sistema se reinicia automáticamente y empieza la instalación. El proceso de instalación

[4] Econometría.- Es una disciplina dedicada al desarrollo de modelos probabilísticos y de métodos de inferencia estadística, teniendo en cuenta la naturaleza de los datos económicos, para el estudio de relaciones económicas. Por ejemplo: estudios de la relación inflación-desempleo, finanzas, campañas electorales, etc.

es largo, pero no necesita demasiada atención y es capaz de aplicar el reconocimiento plug and play (conectar y listo) correctamente si el hardware es 100 % compatible. El reconocimiento del hardware es la parte más larga de la instalación. Una vez terminada la copia de archivos y controladores, el sistema se reiniciará y entraremos en la fase de configuración, creación de accesos y registro de componentes. La personalización y configuración del sistema se puede realizar casi por completo desde el panel de control, incluyendo las opciones de carpetas.

Requisitos de Hardware

En la siguiente tabla mostramos la lista de requerimientos en hardware para cada una de las dos variantes de servidor de Windows 2000:

Componente	Windows 2000 Server	Windows 2000 Advanced Server
Computadora	IBM ó 100% compatible	
Procesador	Intel Pentium 133 Mhz. o equivalente (hasta 4 procesadores)	Intel Pentium 133 Mhz. o equivalente (hasta 8 procesadores)
Memoria RAM	256 Mb	256 Mb
Disco duro	Al menos 1 Gb libre	1 GB libre
Video	VGA o superior	VGA o superior
Controles	Teclado y ratón compatibles	Teclado y ratón compatibles

Windows XP

Windows eXPerienced (eXPerimentado) aparece en dos versiones: Windows Home Edition (Edición Casera) y Windows Professional.

Ambas versiones de Windows incluyen una interfaz fácil de usar y varias mejoras hechas en la forma de trabajar con los archivos y con las unidades de disco. En particular, Windows XP Professional integra funciones para el manejo de unidades grabadoras de disco compacto desde el explorador de Windows, así como la

posibilidad de comprimir/descomprimir archivos en lo que llama carpetas comprimidas, al estilo del software de compresión de archivos Winzip. La versión profesional permite instalar de manera opcional desde el CD-ROM de distribución, un software de servidor de web conocido como IIS (Internet Information Server – Servidor de Información Internet) que se puede activar casi de inmediato como un servicio del sistema; otra opción muy útil es la de manejo de servicios FTP (File Transfer Protocol – Protocolo de Transferencia de Archivos) para compartir ciertas carpetas con algunos usuarios en especial o con todos los usuarios de WEB de forma pública. Al igual que Windows 2000, el sistema operativo Windows XP maneja también la tecnología Plug and Play y a la fecha, mantiene un número elevado de drivers (controladores de dispositivo) que facilita la auto detección de casi cualquier componente estándar. Este sistema cuenta con varios programas asistentes que guían en el proceso requerido para llevar a cabo varias actividades, un ejemplo es la conexión a Internet que resulta muy sencilla de realizar.

Administración del sistema

Tanto en las distintas variantes de Windows 2000 como en Windows XP Professional, la administración global del sistema se realiza a través de un conjunto de herramientas denominado "herramientas administrativas", el cual organiza los recursos, servicios, dispositivos de almacenamiento y seguridad que utilizan tanto en el sistema local como en ordenadores remotos. Básicamente se cuenta con la posibilidad de administrar los siguientes elementos:

- Herramientas del Sistema
- Almacenamiento
- Servicios y Aplicaciones

En Herramientas del Sistema, por ejemplo, disponemos de un visor de sucesos y del Administrador de dispositivos, una síntesis jerarquizada de los dispositivos instalados en el PC que permite hacer modificaciones y búsquedas para resolver conflictos IRQ

(Interrupt ReQuest line – Línea de Petición de Interrupciones) o DMA (Direct Memory Access – Acceso Directo a Memoria). Por otro lado, desde Almacenamiento es posible acceder a las propiedades de las unidades de disco, incluyendo unidades extraíbles, y a sus opciones para verificar, compartir y realizar copias de seguridad. Finalmente, Servicios y Aplicaciones proporcionan información más clara sobre los servicios de red implementados, entre ellos los que ya se han mencionado, tales como FTP, Web, Mail, etc.

Por servicio, podemos entender que se trata de cualquier aplicación que corre en background (Segundo Plano) dentro del sistema operativo y que es independiente de cualquier sesión de usuario que se utilice. En otras palabras, basta con mantener encendido el equipo que tiene instalado el sistema operativo Windows (2000 Server o XP Professional) y las aplicaciones que el sistema tiene catalogadas como servicio y que el administrador ha habilitado, deberán activarse automáticamente sin necesidad de hacer ninguna otra actividad adicional, una vez que se ha configurado correctamente.

2.6 REDES Y COMUNICACIONES

Concepto de Red

Este involucra tres aspectos importantes que son el hardware[5], el software[6] y un sistema de cableado o medio de comunicación. Generalmente, una red, se define como el conjunto de computadoras interconectadas entre sí, mediante un sistema de cableado o medio de comunicación, con la finalidad de compartir información y los recursos incorporados en ella.

[5] Es todo aquello que constituye a la computadora físicamente, es decir es tangible, puede ser teclado, monitor, CPU, tarjeta madre, dispositivos periféricos y tarjetas.
[6] Es aquel que se encuentra constituido por un conjunto de medios de programas que le permiten al usuario explotar al máximo las características o propiedades de una computadora.

Sistema de cableado

Se constituye por un conjunto de medios de comunicación o tipos de cables, cuya característica principal es la de transportar información de cualquier tipo de un punto a otro. Los diferentes tipos que existen son: Cable de par trenzado (UTP, STP), Cable coaxial (RG58, RG59, RG62, y 150 tipos mas), Cable de fibra óptica (multimodo, unimodo). Para emplear correctamente el sistema de cableado deberán considerarse implícitamente los conectores asociados a cada uno de ellos: par trenzado, RJ11, RJ45, RJ12; para cable coaxial se emplean BNC "terminador", BNC CRIMP o de rosca, BNC "T"; para fibra óptica se emplean conectores tipo BNC, ST, FDDI, SMART, y otras unidades se emplean para la organización y distribución de la fibra óptica.

Topologías de Red

Se refiere a la forma geométrica que adquiere la red en base a la distribución física de cada una de las computadoras o bien a la forma en que se distribuye la información por toda la red. Generalmente la topología física la marca el tipo de cableado que se utiliza. Existen diferentes tipos de topología, algunas de ellas son: Topología de bus lineal, de estrella y de anillo (lógica).

Topología de bus lineal

Es aquella que se integra por diferentes computadoras interconectadas a través de un solo canal de comunicación. Esta topología tiene la desventaja de que si falla una estación de trabajo pudiese fallar toda la red, además de que la información tiene poca seguridad al transportarse por el bus, inclusive pueden generarse colisiones o choques de datos. Aunque es relativamente económica y de fácil instalación.

Topología de estrella

Esta topología esta construida por un conjunto de computadoras que se enlazan entre sí por cables independientes y a través de un dispositivo central concentrador o bien puede ser el mismo servidor; desde donde se administra y se controla el paso de la información de una estación a otra. Generalmente se emplea par trenzado como cableado entre estaciones y concentrador, debido a que cada estación es independiente a la otra, la probabilidad de que falle toda la red es remota, además existe seguridad en el paso de la información entre estaciones de trabajo que se conoce el origen y el destino de los datos. Aunque es un poco costosa en su instalación por el número de dispositivos que entrega y también costosa en su mantenimiento.

Topología de anillo

Dicha topología esta constituida por un conjunto de computadoras en las cuales se distribuye la información de manera secuencial desde un punto de origen después de haber pasado por los demás puntos o estaciones de trabajo que existan en la red, es decir se formara un ciclo o bien un círculo donde la información se transmitirá constantemente en un sentido determinado. En esta topología tendremos una conexión lógica y no física de las computadoras que integran la red.

Servidores y sus tipos

Servidor es la computadora que cuenta con todos los recursos de la red e información que se dará a compartir entre todas las estaciones de trabajo, además tendrá el control y la administración y los accesos a dichos recursos. Existen servidores dedicado y no dedicados. En base al recurso que tendrán incorporado se pueden clasificar como: servidor de archivos (disco duro), servidor de impresión (impresora), servidor de comunicaciones (módem), servidor de CD-ROM (una unidad de CD-ROM). El servidor dedicado es aquel que posee todos los recursos de la red y que no puede ser operado o manejado directamente por el usuario. El servidor no dedicado será aquel que

además de contar con todos los recursos de la red, también podrá ser usado como estación de trabajo.

Comunicación en redes

Comunicación: Es el intercambio de mensajes o información entre dos puntos, uno llamado origen o transmisor y el otro llamado destino o receptor, dicho intercambio se lleva a cabo a través de un medio de comunicación; el medio puede ser cualquier tipo de cableado, aire o a través de luz, etc. Básicamente existirán dos tipos de comunicación: de manera directa o punto a punto y de punto a multipunto. También existen modos de comunicación, estas son simplex, half duplex y duplex o full duplex. Además de técnicas o métodos electrónicos de comunicación serial síncrona y comunicación serial asíncrona.

Sistema de comunicación

Es el conjunto de elementos y dispositivos electrónicos de comunicación de datos que se interconectan de alguna forma para lograr el intercambio de información. Algunos elementos importantes en un sistema de comunicación son: el transmisor u origen, el codificador, el canal o medio de comunicación, el decodificador y el receptor.

Backbone de red

Es aquel que se constituye como estructura vertebral o esqueleto principal que une a los nodos principales localizados dentro de la red. Es la propiedad o capacidad de los sistemas para poder interconectarse con otros sin importar el tipo de software y hardware incluido, así como el tipo de tecnología, el tipo de plataforma, el tipo de protocolos, el tipo de conectividad, el cual se constituye por diferentes elementos. Los elementos de conectividad son de 2 tipos locales y remotos. Los primeros son aquellos que están incorporados a las redes mediante cableado directo. Los elementos de conectividad remotos se incorporaran mediante un medio que no utilice cableado, por

ejemplo: microondas terrestres, microondas satelitales, radio enlaces, etc. Algunos ejemplos de elementos de conectividad son el repetidor, el puente, el switch, el ruteador, el hub, el gateway.

Clasificación de redes en base a su tamaño

LAN (Local Area Network – Red de área local). Es un conjunto de computadoras interconectadas entre sí con la finalidad de compartir información, enviar datos, utilizar recursos comunes, etc. Pero su característica principal es que utiliza un área geográfica limitada y que no rebasa una distancia de los 10 Km.

MAN (Metropolitan Area Network – Red de área metropolitana). Conjunto de redes que van interconectadas dentro de un área geográfica considerado para una ciudad, su longitud estará comprendida entre los 10 y los 100 Km., podrán emplearse diferentes medios de comunicación principalmente cableado (VTP, STP, coaxial, fibra óptica) y a menudo terrestres.

WAN (World Area Network – Red de Area Global). Es el conjunto de redes LAN y redes MAN que se interconectaran entre si empleando cualquier medio de comunicación (cableado, microondas, radiofrecuencia, telefonías, etc.). La longitud de una red WAN es impredecible, desde los 100 Km. en adelante y puede encontrare en un país, en el enlace de 2 países o más, en la interconexión de 2 continentes o a nivel mundial.

2.7 SEGURIDAD

Definición de riesgo de seguridad

A medida que evolucionan los sistemas de TI, también lo hacen las amenazas a la seguridad que éstos pueden sufrir. Para proteger el entorno de forma eficaz contra los ataques, es necesario conocer con detalle los peligros que se pueden encontrar. Al

identificar las amenazas a la seguridad, se deben tener en cuenta dos factores principales: los tipos de ataques que seguramente se sufrirá y los lugares donde pueden tener lugar.

Muchas organizaciones no tienen en cuenta el segundo factor, pues asumen que un ataque grave sólo puede venir del exterior (normalmente, a través de su conexión a Internet). Muchas empresas pueden no estar al corriente de que se están dando ataques internos, básicamente porque no comprueban si existen.

En octubre de 2001, Microsoft lanzó una iniciativa denominada **STPP** (Strategic Technology Protection Program - Programa Estratégico de Protección de Tecnología). El objetivo de este programa es integrar los productos, los servicios y el soporte de Microsoft dedicados a la seguridad. Microsoft divide el proceso de mantener un entorno seguro en dos fases relacionadas: implementar la seguridad y mantener la seguridad.

Administración de riesgos

No existe un entorno de TI totalmente seguro. Al examinar el entorno, se deberá evaluar los riesgos que sufre actualmente, determinar un nivel de riesgo aceptable y mantener el riesgo a ese nivel o por debajo del mismo. Los riesgos se reducen aumentando la seguridad del entorno. Para entender los principios de la administración de riesgos, es necesario entender algunos términos básicos utilizados en el proceso de los mismos. Éstos incluyen recursos, amenazas, vulnerabilidades, explotaciones y contramedidas.

Recursos: un recurso es cualquier elemento del entorno que intente proteger. Puede tratarse de datos, aplicaciones, servidores, ruteadores e incluso personas. El objetivo de la seguridad es evitar que los recursos sufran ataques.

- Amenazas: una amenaza es una persona, un lugar o un elemento que puede tener acceso a los recursos y dañarlos.

- Vulnerabilidades: una vulnerabilidad es un punto en el que un recurso es susceptible de ser atacado. Se puede interpretar como un punto débil.

- Explotación: una amenaza que se aprovecha de una vulnerabilidad del entorno puede tener acceso a un recurso. Este tipo de ataque se denomina explotación.

- Contramedidas: las contramedidas se aplican para contrarrestar las amenazas y vulnerabilidades y de este modo reducir el riesgo en el entorno.

Administrar la seguridad con la Directiva de Grupo de Windows 2000 Server

Una vez determinado el nivel de riesgo apropiado para el entorno y establecida la directiva de seguridad general, deberá empezar a asegurar el entorno. En un entorno basado en Windows 2000, esto se lleva a cabo principalmente por medio de la Directiva de grupo.

Muchos de los valores de configuración de la seguridad se definen en Windows 2000 a través de la Directiva de grupo, cuyo fin es controlar el comportamiento de los objetos en el equipo local y en el servicio de directorio Active Directory.

Asegurar servidores basándose en su función dentro del entorno Windows 2000 Server

Se deben tener en cuenta también las directivas de línea de base que pueden definirse para todos los servidores miembros y controladores de dominio de la organización, y otras modificaciones que se pueden aplicar a funciones específicas del servidor.

Este enfoque permite que los administradores bloqueen los servidores por medio de directivas de línea de base centralizada, aplicadas de forma coherente a todos los servidores de la organización. Las directivas de línea de base sólo permiten una funcionalidad mínima, pero sí permiten que los servidores se comuniquen con otros

equipos en el mismo dominio y su autenticación a través de los controladores de dominio. A partir de este estado más seguro, se pueden aplicar otras directivas incrementales más, que permiten que cada servidor realice únicamente las tareas específicas definidas por su función. La estrategia de administración de riesgos determinará si es apropiado para el entorno que se lleven a cabo estos cambios.

Lo nuevo en seguridad para Windows XP

Windows XP ofrece la versión más confiable de Windows con las mejores funciones de seguridad y privacidad que Windows haya ofrecido hasta ahora. Sobre todo, se ha mejorado la seguridad en Windows XP para ayudarle a tener una experiencia de cómputo segura y privada.

Windows XP es el sistema operativo de elección para negocios de todos tamaños, y ofrece los servicios de seguridad más confiables para el cómputo empresarial. Windows XP incluye las funciones de seguridad que necesita para el trabajo en red y seguridad empresarial. Estas funciones de seguridad ofrecen nuevas capacidades de administración que reducirán los costos en informática y permitirán desarrollar servicios y soluciones seguras.

Mejoras en la seguridad

Windows XP incluye un número de funciones que los negocios pueden utilizar para proteger archivos, aplicaciones y otros recursos seleccionados. Estas funciones incluyen listas de control de acceso, grupos de seguridad y políticas de grupo además de las herramientas que permiten a los negocios configurar y administrar estas funciones. Juntas ofrecen una infraestructura de control de acceso poderoso, con flexibilidad, para redes empresariales.

Windows XP ofrece cientos de configuraciones relacionadas con la seguridad que se pueden implementar individualmente. El sistema operativo Windows XP también

incluye plantillas predefinidas de seguridad, las que pueden implementar los negocios sin necesidad de hacer modificaciones o utilizarlas como la base de una configuración de seguridad más personalizada. Los negocios pueden aplicar estas plantillas de seguridad cuando:

- Creen un recurso, tal como una carpeta o archivo compartido, y ya sea que acepten las configuraciones de lista de control de acceso por predeterminación o implementen configuraciones de listas de control de acceso personalizado.

- Coloquen usuarios en los grupos de seguridad estándar, tales como Usuarios, Usuarios avanzados y Administradores, y acepten las configuraciones ACL predeterminadas que aplican a dichos grupos de seguridad.

- Utilicen las plantillas de Políticas de grupo Básica, Compatible, Segura y Altamente segura que se han incluido con el sistema operativo.

Acceso controlado a la red

Windows XP ofrece seguridad integrada para mantener alejados a los intrusos. Esto se realiza al limitar a cualquiera que trate de tener acceso a la computadora de una red hacia los privilegios del nivel "huésped". Si los intrusos tratan de acceder al equipo y obtener privilegios no autorizados tratando de adivinar las contraseñas, no tendrán éxito u obtendrán únicamente acceso de nivel huésped limitado.

Administración de la autenticación de la red

Un número cada vez mayor de sistemas basados en Windows XP están conectados directamente a la Internet más que a los dominios. Esto hace que la administración adecuada del control de acceso (incluyendo contraseñas duras y permisos asociados con diferentes cuentas), sea más importante que nunca antes. Para asegurar la seguridad, necesita personalizar las configuraciones de control de acceso

relativamente anónimas comúnmente asociadas con ambientes abiertos de Internet. Como resultado, las funciones predeterminadas en Windows XP requieren que todos los usuarios se conecten en la red para utilizar la cuenta huésped. Este cambio está designado para evitar que los piratas traten de tener acceso a un sistema a través del Internet al conectarse utilizando una cuenta local de Administrador que no tiene contraseña.

Uso compartido simple

Por predeterminación, en los sistemas Windows XP que no están conectados a un dominio, todos los intentos para conectarse a través de la red estarán forzados a utilizar la cuenta huésped. Además, en las computadoras que utilizan un modelo de seguridad de uso compartido simple, el cuadro de diálogo Propiedades de Seguridad se reemplaza por un cuadro de diálogo simplificado 'Propiedades de documentos compartidos'.

Restricción de contraseña en blanco

Para proteger a los usuarios quiénes no tienen protegidas sus cuentas con contraseña, las cuentas Windows XP sin contraseña se pueden utilizar únicamente para conectarse en una consola de computadora física. Por predeterminación, las cuentas con contraseñas en blanco no se pueden utilizar para conectarse a la computadora de manera remota en la red, o para cualquier otra actividad de registro excepto en la pantalla de registro de la consola física principal. Por ejemplo, no puede utilizar el servicio de registro secundario para iniciar un programa como un usuario local con una contraseña en blanco.

Asignar una contraseña a una cuenta local elimina la restricción que evita la conexión sobre una red. Esto también permite que la cuenta tenga acceso a todos los recursos para los que tenga acceso autorizado, aun en una conexión en red.

Esta restricción no aplica a las cuentas de dominio. Tampoco aplica a la cuenta de huésped local. Si la cuenta de huésped está habilitada y tiene una contraseña en blanco, esto permitirá la conexión y acceso a cualquier recurso autorizado para acceso por medio de la cuenta del huésped.

Sistema de encriptación de archivos

La funcionalidad aumentada del Sistema de encriptación de archivos (EFS) ha mejorado de manera importante el poder de Windows XP al ofrecer flexibilidad adicional para usuarios corporativos cuando implementan soluciones de seguridad basadas en archivos de datos encriptados.

Firewall de conexión a Internet

El Firewall de conexión a Internet (ICF) en Windows XP ofrece a los escritorios y computadoras móviles protección de las amenazas de seguridad cuando utilizan DSL, módem de cable, o conexiones por modem de marcación a un Proveedor de servicio de Internet (ISP).

Configuraciones de políticas de grupo relacionadas con la seguridad

Windows XP incluye plantillas de seguridad, colecciones preconfiguradas de políticas relacionadas con seguridad que se pueden utilizar para asegurar el nivel adecuado de seguridad en las estaciones de trabajo. Estas plantillas representan configuraciones de seguridad estándar bajas, medias y altas, y se pueden personalizar para cumplir las necesidades de seguridad específicas.

También puede establecer políticas de seguridad para artículos de administración de contraseña, tales como:

- Determinar longitudes mínimas de contraseña.

- Establecer el intervalo entre los cambios de contraseña requeridos.

- Controlar el acceso a recursos y datos.

CAPÍTULO III
PLANTEAMIENTO DEL PROBLEMA Y PROPUESTA DE SOLUCIÓN

3.1 PROBLEMÁTICA ACTUAL

Actualmente se llevan a cabo tres procesos principales en la operación del área de seguridad del ISP, y los cuales son ejecutados de forma manual, siendo el principal objetivo del sistema la automatización completa de los procedimientos para evitar posibles errores u omisiones.

Procedimiento de inventario de usuarios de la red

Las figuras 3.1.1, 3.1.2 muestran el proceso para controlar el inventario de los usuarios y perfiles que tienen acceso a las plataformas de equipos de red.

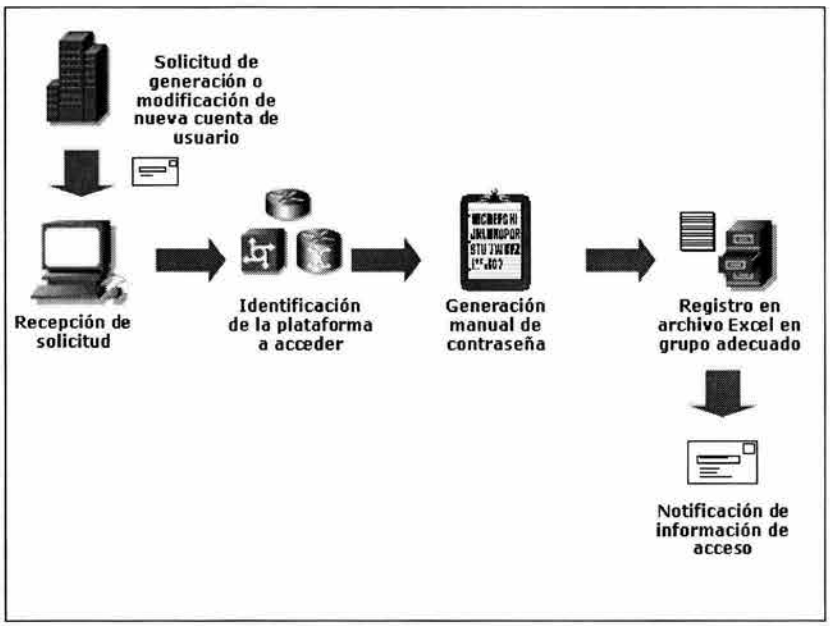


Figura 3.1.1 Procedimiento de inventario de cuentas de usuario

- Solicitud de cuenta de usuario. Cuando una persona ingresa a laborar a las áreas de operación de red de la empresa, ésta deberá contar con un usuario personalizado para acceder a las plataformas de equipos de red existentes en la

infraestructura, y las cuales se tienen en los inventarios. La información que se le entrega al personal es su nombre de usuario, su o sus contraseñas, y se le informan los permisos que tendrá dependiendo del perfil al que se ingrese. Las áreas de operación solicitan al área de seguridad la asignación de esta nueva cuenta.

Para el caso en que se solicita una modificación de cuenta de usuario, puede deberse al deseo de cambiar las contraseñas de acceso de una determinada persona, o bien la modificación del perfil al que esta cuenta pertenece. La solicitud que se recibe por correo es similar para ambos casos.

- Identificación de la plataforma. De acuerdo al área y funciones del usuario se identifican la o las plataformas a las que debe tener acceso, y de acuerdo a esta plataforma se actualiza su información en los archivos correspondientes a cada una de ellas.

- Generación de contraseñas. El usuario contará con una o dos contraseñas para acceder a alguna plataforma en específico, estas contraseñas deben cumplir con las políticas establecidas por la empresa, por lo que su generación dependerá de ello. Estas contraseñas son generadas de forma manual y almacenadas en los archivos de inventarios de usuario para futuros usos, como puede ser la notificación de contraseñas a un usuario que no las recuerda.

- Registro. Una vez teniendo los datos del solicitante, la plataforma y las contraseñas generadas se procede a su registro en los archivos de Excel de toda esta información que consta básicamente de nombre completo, nombre de la cuenta de usuario, contraseña o contraseñas y perfil al que pertenece.

- Notificación de información de acceso. Se genera manualmente un correo electrónico de notificación indicándole al usuario su información de acceso, y

donde además se le advierte sobre las consecuencias que se tendrían en caso del mal uso de la cuenta.

El proceso de modificación o alta de nuevos perfiles de usuarios, depende de la plataforma, del área de operación y de las funciones que esta debe tener. En la figura 3.1.2 se muestra el proceso de actualización de perfiles de usuario, en base a los aspectos anteriores.

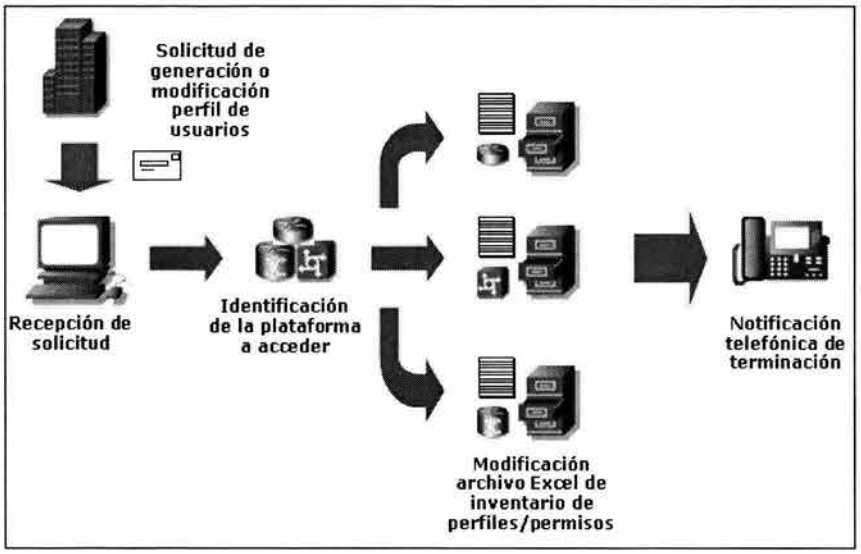


Figura 3.1.2 Administración de inventario de perfiles y permisos de usuarios

- Solicitud de generación o modificación de perfil. La información contenida en esta solicitud es el nombre del área de operación que hará uso de él, las funciones de la misma, y los usuarios que estarán contenidos en este perfil. Esta solicitud es recibida vía correo electrónico.

- Identificación de plataforma. Para fines de identificación del archivo a modificar, es importante saber a qué plataformas se tendrá acceso, debido a que cada una de ellas contendrá el perfil correspondiente al área en cuestión.

- Modificación de archivos. El control de esta información es llevada en archivos de Microsoft Excel, el cual contiene la información del grupo, el área a la que pertenece y los permisos de usuarios.

- Notificación de terminación. Debido a que en esta actividad no se regresa ningún tipo de dato al solicitante, solamente se le notifica telefónicamente que ya puede hacer uso de sus cuentas de usuario. Los permisos los verá reflejados en sus actividades diarias.

Procedimiento de inventario de equipos de red

La figura 3.1.3 muestra el proceso que se sigue para administrar el inventario de los equipos de red que forman la infraestructura.

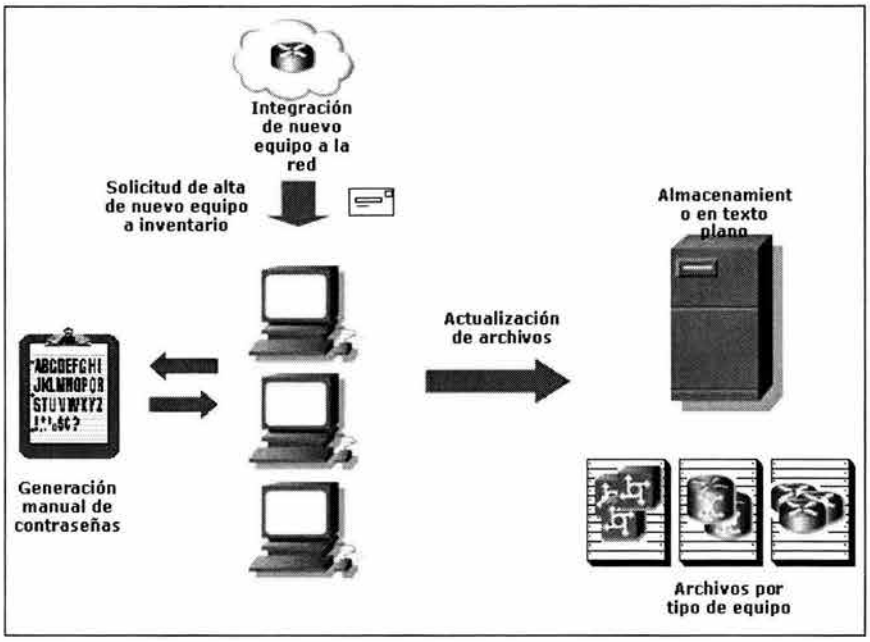


Figura 3.1.3 Procedimiento de inventario de equipos

- Integración de nuevo equipo a la red. Las áreas de ingeniería y configuraciones del ISP conectan y ponen en funcionamiento un nuevo equipo de red, que puede

tratarse de un nuevo ruteador, LAN switch, servidor de acceso, etc. Al terminar de recibir el equipo, estas áreas informan al área de seguridad de red el nombre del equipo, la dirección IP y el tipo o plataforma para proceder a contemplarlo en los archivos de texto de inventarios, mediante una solicitud de integración del equipo a los inventarios.

- Recibida la solicitud de integración a inventarios mediante un correo electrónico se procede a dar de alta el equipo en los archivos de texto. Existe un archivo de texto independiente dependiendo del tipo o plataforma del nuevo equipo. Con el dato de tipo o plataforma del equipo, se selecciona el archivo que va a ser actualizado. Dentro del archivo se especifica el nombre el equipo y su dirección IP.

- Generación manual de contraseñas. Para los equipos que requieran la configuración de una o dos contraseñas de acceso a él, éstas se generan de manera manual considerando las políticas y recomendaciones de la empresa para la generación de las mismas.

- Almacenamiento en texto plano. Una vez que se realiza la actualización de los archivos, la información queda almacenada en texto plano, un archivo por cada plataforma, y en cada archivo la lista de los equipos con su nombre y su dirección IP.

Las áreas de la empresa que requieran acceso a los inventarios, lo podrán hacer mediante la conexión por telnet al servidor de los inventarios, y haciendo una búsqueda del equipo del que requieren conocer información. Esta información puede ser general, simplemente la consulta del total de equipos considerados en el inventario por plataforma, o bien, más específica, como la dirección IP o las contraseñas configuradas en algún equipo específico, si es el caso.

Procedimiento de seguimiento y solución de incidentes de seguridad

La figura 3.1.4 nos muestra el proceso que actualmente se sigue para atender y solucionar un incidente de seguridad.

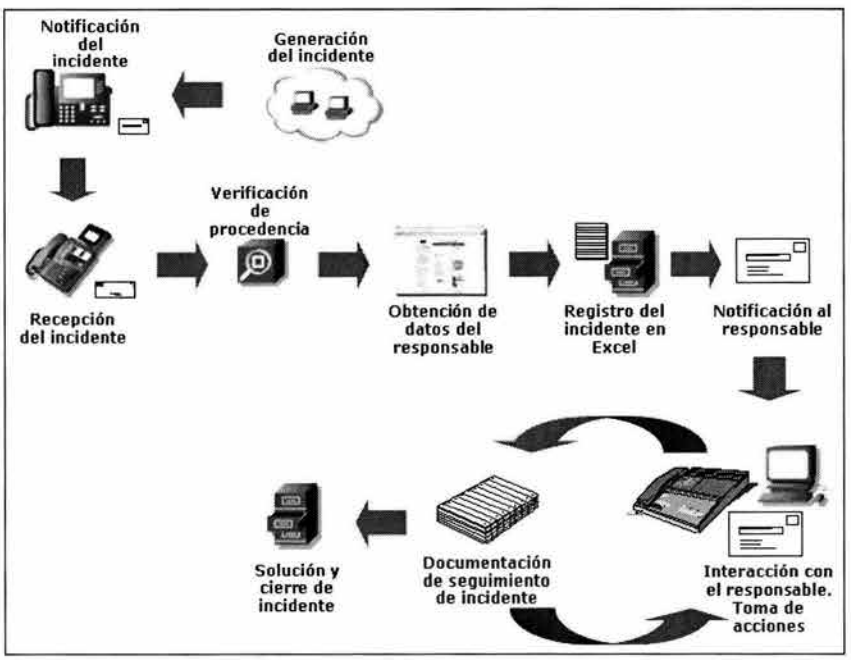


Figura 3.1.4 Seguimiento de incidentes de seguridad

- Generación del incidente. Es la acción mediante la cual se realiza un mal uso de los recursos de red que el ISP asigna a sus clientes, y que pueden ser intencionales o no intencionales. Los tipos de incidentes van desde el simple envío de un correo ofensivo, un rastreo de puertos o una intrusión en redes y sistemas sin los permisos correspondientes, pudiendo obtener información confidencial de alguna organización. El tipo de incidente es identificado una vez que se recibe el reporte correspondiente. De acuerdo a la asignación de direcciones IP con que cuenta el ISP, se puede identificar cuando se trata de un incidente de un cliente propio o bien de algún usuario externo totalmente a la organización, como son clientes de otros ISP o bien hasta provenientes de otros países.

- La notificación y recepción del incidente puede ser por vía telefónica o bien por correo electrónico, especificando los datos del generador del incidente, como es la dirección IP origen del incidente, la fecha y hora a la que ocurrió y el tipo de actividad que se presentó.

- Verificación de la procedencia. Consiste en la verificación mediante la cual se realiza una traza[7] a la dirección IP para comprobar los equipos de red a los que está conectado y cual de los equipos pertenecientes a la infraestructura de red del ISP es el más próximo a esta dirección. De este proceso se obtiene el nombre del último ruteador del ISP y el ruteador siguiente a éste y que comunica con la IP fuente del incidente.

- La obtención de datos del responsable de la IP origen se realiza mediante la obtención de información de contacto técnico a través de las páginas de asignación de dominios y direcciones IP mundiales o regionales, en donde nos indiquen el país, organización, contacto técnico, teléfono y dirección de correo electrónico.

- El registro del incidente se hace en una hoja de Microsoft Excel que tiene cada operador en su equipo de trabajo y que al final del mes es conjuntado con los archivos de los demás operadores. En este archivo se guarda en cada columna la información recopilada en el proceso de obtención de datos. Cuando se soluciona un incidente, éste es marcado en la hoja de cálculo.

- Una vez que se cuenta con la información de la organización responsable y contacto técnico, se procede a enviarle una notificación vía correo electrónico, indicándole los pormenores del incidente. Este proceso se ejecuta de manera manual y por cada uno de los incidentes presentados.

[7] Una traza o traceroute es una utilería que verifica el trayecto que un paquete de información de red sigue para llegar a un equipo en Internet, mostrando el número de saltos que el paquete requiere para llegar al destino y cuanto tiempo se toma en hacer cada salto. Windows incluye está herramienta y se ejecuta mediante el comando tracert especificando la dirección IP destino.

- Interacción con el responsable, en la cual se establece contacto con él y a través de recomendaciones nuestras se realizan acciones que contribuyan a la solución del incidente, las cuales pueden constar de acciones restrictivas de tráfico, o bien aplicación de parches a los sistemas involucrados.

- Conforme se va interactuando con el contacto técnico responsable y se van aplicando acciones, éstas se van documentando en la hoja de Excel en la que se van levantando los casos, en la última columna de los datos del incidente.

- Una vez que se llega a la solución del incidente, se procede a cerrar el caso. Se le pone una marca al renglón de la base de datos donde este incidente fue levantado, que consta generalmente el cambio de color de fondo del renglón o renglones involucrados.

3.2 REQUERIMIENTOS GENERALES Y PARTICULARES

Requerimientos generales

Las áreas involucradas en el proceso de la operación de la red, son las mostradas en la figura 3.2.1.

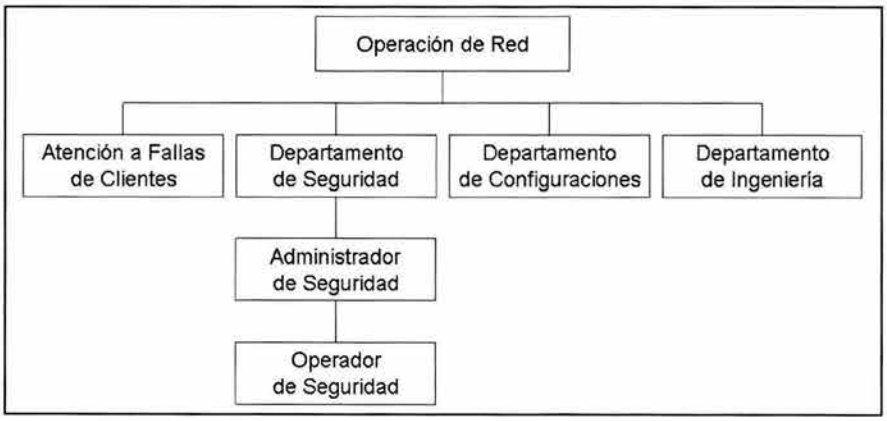


Figura 3.2.1 Organización de la Subdirección de operación de red

- Atención a Fallas de Clientes. Se encarga de recibir y clasificar los reportes de fallas en general de los clientes que tienen contratado algún servicio; los reportes clasificados como incidentes de seguridad, son canalizados al Departamento de Seguridad.

- Departamento de Seguridad. Se encarga de dar seguimiento y solución a los incidentes de seguridad turnados por atención a clientes, por solicitud directa de los clientes o usuarios de Internet.

    - Administrador de Seguridad. Se encarga de planificar y organizar la estrategia de seguridad, involucra la atención a incidentes, la administración de usuarios, la asignación de permisos y la administración de equipos de red.

    - Operador de Seguridad. Pone en práctica la estrategia de seguridad establecida por el administrador.

- Departamento de Configuraciones. Recibe del Departamento de Ingeniería la notificación de instalación de nuevos equipos integrados a la red para que esta comience con su configuración.

- Departamento de Ingeniería. Asigna e instala físicamente los nuevos equipos integrados a la red, poniéndoles su configuración básica. En caso de fallas en equipos ya existentes, realiza una inspección física del equipo y detecta el problema.

Se requiere de una atención rápida de los incidentes de seguridad, así como la generación de bitácoras de administración de equipos de red en el menor tiempo posible, asignación de cuentas de usuario personalizadas para el personal y su organización en perfiles de acuerdo a su nivel y a su función, esquema de notificación

automática de eventos (incidentes de seguridad, información de cuentas de acceso y boletines). Todo esto contenido en un sistema amigable y multiusuario que deberá ser operado por el área de seguridad y que presente una interfaz de usuario similar al ambiente Windows, integrándose totalmente a él, que en su uso cotidiano permita reducir tiempos de operación y espera de las áreas solicitantes, así como minimizar posibilidades de error instalándose en terminales que se conectarán a una base de datos central. Adicionalmente se requiere la generación de reportes de operación mensual.

Requerimientos particulares

El sistema deberá ser manipulado por todo el personal del área de seguridad de la empresa, para agilizar las respuestas a los requerimientos de las áreas con las que se involucra el Departamento. Debido a ello, el sistema deberá ofrecer las siguientes características:

Interfaz de usuario

- El sistema deberá contar con una interfaz de usuario que posea una ventana principal, donde se verá el contenido de los inventarios en forma de árbol, y en el cual se tendrá como elementos principales la Administración de Usuarios, la Administración de Equipos de Red y las Notificaciones de Seguridad. A partir de ellas dependerá toda la información almacenada en la base de datos.

- La ventana principal constará de dos paneles. En el primero de ellos se mostrará el árbol de elementos del sistema de Administración de Seguridad Informática y en el segundo, los elementos incluidos en el nodo seleccionado en el primer panel.

- Existirá una barra de herramientas superior, que permitirá el acceso rápido a las principales funciones del sistema, indicadas mediante íconos y textos descriptivos de cada una.

- Adicionalmente contará con una barra de menús, en los cuales estarán incluidas todas las funcionalidades del sistema, incluyendo las especificadas en la barra de herramientas.

- El sistema será accedido por medio del usuario Administrador y su contraseña, la cual podrá ser configurada en cada cliente donde la aplicación se encuentre instalada. La contraseña de acceso no tiene que ser forzosamente la misma en todas las terminales, cada operador podrá establecer la contraseña de forma individual en su terminal.

Administración de inventario de usuarios

- Generar grupos de usuarios de acuerdo al área y nivel de jerarquía que tienen, así como a la plataforma de equipos de red a la que tendrán acceso, de acuerdo a la plataforma manejará la opción de incluir el inventario de los permisos que tendrá cada uno.

- El registro de usuarios se hará considerando los siguientes datos: Nombre completo, nombre de usuario, contraseña(s), correo electrónico y observaciones.

- Las contraseñas de acceso de los usuarios se generaran de manera aleatoria y alfanumérica por política de la empresa, el sistema será capaz de generar dichas contraseñas utilizando los caracteres de la 'a' a la 'z' en minúsculas y mayúsculas, los números del '0' al '9' y los caracteres especiales '#', '$', '!', '%' y '&', con una longitud mínima de 8 caracteres. Se contará con la opción de generar la contraseña de forma manual.

- Deberá contemplar la encriptación de la contraseña mediante una llave, que no conocerá el usuario, la cual se almacenará en el registro del usuario y que será necesaria para obtener la contraseña en caso de ser requerida.

- Será necesario un mecanismo de notificación automática de contraseñas a través de correo electrónico, una vez que la cuenta sea generada con todos sus parámetros y configurada en la plataforma correspondiente; indicando el nombre de usuario, la o las contraseñas y una advertencia de uso indebido de la cuenta.

- Contendrá un módulo de envío masivo de contraseñas, mediante el cual se hará un envío a todos los usuarios de una plataforma especifica, y que será útil para los casos en que todos los usuarios de una plataforma tengan que ser actualizados.

Administración de inventarios de equipos de red

- Permitirá integrar grupos de equipos de acuerdo a su función y servicios que ofrecen, teniendo la opción de almacenar información de contraseñas locales configuradas en ellos.

- Para los equipos que requieran contraseñas de acceso local estas deberán ser generadas aleatoria y alfanuméricamente y con las especificaciones de las contraseñas de acceso de los usuarios.

- En el registro de un equipo se almacenará el nombre del mismo dentro de la red, su dirección IP, el grupo al que pertenecen y la fecha en la que son registrados en el inventario. Esta fecha será tomada automáticamente del sistema cuando se realice la inserción del registro en la base de datos. Adicionalmente se tendrán dos campos para almacenamiento de contraseñas en caso de equipos que requieran acceso local, incluyendo una más para la llave de encriptación.

- La interfaz de usuario para especificar los datos de un equipo en la red, permitirá hacer un verificación de conectividad hacia el equipo, para asegurar que sea alcanzable al momento de integrarlo al inventario.

- Se permitirá la edición de los registros de los equipos, para los casos en los que sea necesario cambiar la dirección IP o el nombre del mismo, así como para casos en los que el equipo cambie de grupo de trabajo.

- El sistema contendrá una opción de importación de archivos de texto para realizar integraciones masivas, útil cuando se desee integrar al inventario una lista larga de equipos que por su extensión pueda incrementar la captura unitaria de ellos. El formato del archivo de texto, será el utilizado con anterioridad a la existencia del sistema, es decir, el nombre del equipo, su dirección IP y contraseñas, si existen, separados por dos puntos.

- Existirá la opción de exportación a archivos de texto, en el cual se especificará la plataforma de equipos, y se generará un archivo con el formato especificado en la opción de importación. Está opción será útil para el caso de la generación de respaldos de información adicionales a los manejados por Microsoft SQL 2000 para la totalidad de la base de datos.

Administración de incidentes de seguridad

- Los casos de incidentes de seguridad serán dados de alta una vez recibido el reporte de alguna entidad externa, capturando la información de la dirección IP de origen del incidente, nombre y dirección IP del último ruteador de la infraestructura a través de la cual se conecta a la red, la dirección IP del ruteador externo, fecha y hora del incidente, tipo, nombre de la organización responsable de la IP, contacto técnico, dirección de correo electrónico y teléfono. Adicionalmente contendrá un campo de control para establecer su estado.

- Los estados por los que pasará un incidente de seguridad y que podrá ser cambiado a través del sistema será atendido, y cerrado o solucionado, y será almacenado en la tabla de incidentes de seguridad a través de un campo de tipo booleano.

- Los incidentes de seguridad serán notificados automáticamente a los responsables de las direcciones IP involucradas, una vez capturados todos los datos anteriores, mediante una opción que permita el de notificaciones. Se enviarán todas las notificaciones que no hayan sido enviadas con anterioridad.

- En caso de presentarse otro incidente para una determinada dirección IP ya registrada previamente, mostrará automáticamente toda la información referida del caso anterior, teniendo que capturar únicamente la fecha, hora y tipo de incidente para el nuevo caso.

- Permitirá la opción de documentación del incidente en un campo llamado Comentarios, en el cual se escribirán los avances por los que el incidente vaya pasando durante la solución del mismo.

Notificaciones de seguridad

- Tendrá un modulo de envío de notificaciones de seguridad vía correo electrónico y de manera masiva con la información de nuevas recomendaciones, aparición de nuevos virus y aplicación de nuevos parches a los sistemas.

- El módulo de notificaciones tendrá la opción de almacenarlas en la base de datos del sistema para futuras referencias, como por ejemplo, si se desea hacer el envío de una misma notificación en diferentes fechas y horas, evitando así la reescritura completa de la misma.

- Existirá la opción para los casos en los que se desee hacer un envío masivo de cierta notificación, y que deba ser enviada a toda una plataforma de usuarios, recolectando las direcciones de correo de cada uno de ellos de la base de datos y enviando la notificación por cada cuenta de forma automática, sin tener que

capturar el mensaje nuevamente para cada uno de ellos, o bien, evitar agregar manualmente cada dirección de correo en el envío del mensaje.

Módulo de búsquedas

El sistema incluirá una opción de búsqueda para usuarios, equipos registrados o incidentes de seguridad.

- En la búsqueda de usuarios registrados en la base de datos, podrá especificarse una cadena que podrá estar contenida en los campos de nombre completo, nombre de usuario o dirección de correo electrónico. Los búsqueda se realizará sobre la plataforma especificada en las opciones de búsqueda; si no se especifica entonces se hará sobre todas las plataformas de usuario existentes en el sistema, y en los resultados se mostrarán los coincidencias encontradas con la información de nombre de usuario, nombre completo, plataforma y grupo o perfil.

- La búsqueda de equipos registrados, se realizará ya sea por dirección IP o parte de ella o por el nombre que tiene el equipo en la red. Adicionalmente podrá especificarse la plataforma de equipos. En los resultados se mostrará la IP del equipo, su nombre de red, la fecha de alta y el grupo de trabajo donde se encuentra.

- Los incidentes de seguridad permitirán la búsqueda por dirección IP fuente del incidente, organización, contacto técnico o correo electrónico del contacto técnico, además del tipo de incidente.

Para todas las opciones de búsqueda podrá especificarse adicionalmente el parámetro fecha, que indicará un rango de fechas en el cual se registró la información que se está buscando en la base de datos del sistema.

Reportes

De acuerdo a la operación del sistema, se tendrá un módulo de reportes en los cuales se observarán las actividades realizadas. Todos los reportes tendrán la característica de ser generados mensualmente y de manera comparativa desde el primer mes del año en curso hasta el presente, indicando en cantidades las operaciones que han sido efectuadas en los módulos de administración de usuarios, administración de equipos, atención a incidentes de seguridad y notificaciones automáticas. Los reportes que se tienen en consideración son los siguientes:

- Reporte de Operaciones del Departamento de Seguridad de Red, en el cual serán enumeradas todas las actividades que se han realizado, mostrando los valores numéricamente. Se mostrará en forma de tabla y se incluirá una breve descripción de las cada una de las actividades. Cada actividad deberá tener un identificador.

- Reporte General de Inventario de Equipos, en el que se mostrará mensualmente la totalidad de equipos que fueron ingresados o dados de baja de los inventarios del sistema.

- Reporte de Integración a los Inventarios de Equipos por Plataforma, que mostrará todos los equipos que fueron dados de alta en los inventarios de equipos, especificando el valor numérico por cada una de las plataformas existentes en el sistema.

- Reporte de Administración de Perfiles de Usuario. Para los grupos de usuarios en donde la plataforma requiere que se especifiquen permisos para cada uno, se llevará un control de las veces en que un grupo es modificado. Esta información numérica será mostrada en este reporte únicamente.

- Reporte de Administración de Cuentas de Usuario. En el que se mostrará la cantidad de usuarios que fueron dados de alta, dados de baja o modificados en el inventario.

- Reporte de Incidentes de Seguridad por Tipo de Amenaza. Se mostrará el total de los incidentes de seguridad que se atendieron por los operadores de seguridad y que fueron documentados en sistema. La información será incluida de forma numérica total y en porcentaje, por cada tipo de incidente presentado.

- Reporte de Incidentes de Seguridad. Mostrará el total de incidentes de seguridad que se atendieron y documentaron, en total, sin importar el tipo, incluyendo la información de cuantos se atendieron y cuantos se solucionaron.

Todos los reportes anteriores se generarán mensualmente y contarán con las siguientes características:

- Contendrán un identificador por tipo de reporte que estará formado por el tipo, el año al que hacen referencia y la fecha en la que corresponde la generación al principio de cada mes.

- Contarán con objetivo, desarrollo, detalle de la información y observaciones.

- El objetivo y la descripción del desarrollo es diferente para cada reporte, pero igual para el mismo tipo de reporte a través de su generación mensual.

- El detalle de la información mostrada se hará en una tabla con la información para cada uno de los meses desde el primero del año hasta el actual, indicando para cada mes su valor numérico. Se obtendrá al final del reporte el promedio mensual de la actividad a la que se refiere el reporte.

- Las observaciones si podrán variar mes con mes para un mismo reporte y serán anotadas al momento de generar el mismo.

- Los reportes serán generados desde la aplicación para los administradores de seguridad y su formato es HTML. Para otras áreas en el que se deseen tener los estadísticos, serán obtenidos a través de un servidor Web, mediante una página, en la cual podrán acceder con un usuario y contraseña, que será administrado por el área de seguridad a través del sistema como una plataforma de usuarios independiente.

Bitácoras

Las bitácoras de operación de equipos de red, serán generadas para la plataforma de usuarios con acceso a equipos con autentificación por servidor TACACS+, y las cuales son almacenadas en un servidor Cisco Secure[8] y el cual tiene almacenadas en un directorio FTP las bitácoras de operación en texto plano, con cada campo separado por comas.

El análisis y formato de las bitácoras será ejecutado por sistema, y contará con un módulo de conexión por FTP al servidor Cisco Secure, que tomará como entrada estas bitácoras en texto plano y tomará los campos de fecha, dirección IP del equipo accedido, el nombre en la red del equipo, el usuario y el comando que ejecutó.

Las bitácoras podrán ser generadas por equipo (especificando su dirección IP), por usuario, por comando ejecutado en el equipo o parte de él y por fecha, permitiendo cualquier combinación entre ellos. Se realizará la búsqueda de acuerdo a los parámetros especificados y el archivo de salida estará integrado por todas las coincidencias que sean encontrada de acuerdo a éstos.

[8] Cisco Secure es una aplicación de servidor que ofrece una solución de identificación de red centralizada y una administración de usuarios simplificada para diferentes tipos de dispositivos de red Cisco. Se usa para administrar acceso de usuarios, ruteadores y dispositivos CISCO.

El nombre del archivo se generará en base a lo especificado en los parámetros de búsqueda, adicionándole el prefijo CSLogResult y cada parámetro de búsqueda separado por guiones.

3.3 RECOPILACIÓN Y ANÁLISIS DE LA INFORMACIÓN

Administración de perfiles y usuarios

En el caso de los archivos de registro de perfiles y usuarios se manejan dos clasificaciones; la primera establece la categoría del usuario y la segunda el grupo de trabajo al que se le integra. Una parte de la lista se presenta en el par de tablas 3.3.1.

CATEGORÍAS
Becario
Staff
Junior
Senior
Supervisor
Subgerente
Gerente
Subdirector

GRUPOS DE TRABAJO	
IntConfiguraciones	NO Expiración
IntFallasClientes	Restricciones a equipo
IntFallasDorsal	Restricciones a equipo
IntUniProblemas	ssr-prove
IntUniSeguridad	MCEsRouters
IntUniSGestion	ADSLNoexpire
C.Tecnologico	Uninet - internet
UniFallasClientes	Uninet - internet
UniFallasDorsal	Soporte Dorsal
ConfigUninet	Soporte Problemas
UniIntDesarrollo	Soporte HP
UniIntIngerieria	CISCO
Externos Nivel Exec	Externos Nivel Enable

Tabla 3.3.1 Pareja de tablas para clasificar a los usuarios de la red.

Además de las tablas anteriores, se utiliza otra que contiene la lista de comandos de red que puede utilizar cada usuario según la categoría y grupo al que pertenece. De esta forma se tiene un control estricto sobre las actividades que realiza cada usuario en el ámbito de la red del ISP. En la tabla 3.3.2 se muestra la relación de comandos que

se han mencionado, en ella se incluyen las que explícitamente permiten ejecutar una acción o bien que de forma explícita la inhiben.

permit configure terminal	permit line	permit no half-duplex	permit transport
permit interface	permit logging	permit no line	permit no transport
permit ip	permit login	permit no accounting	permit framing
permit controller	permit password	permit no authorization	permit no framing
permit terminal	permit autobaud	permit no logging	permit channel-group
permit clear	permit speed	permit no login	permit no channel-group
permit show	permit telnet	permit no autobaud	permit frame-relay
permit description	permit timeout	permit no monitor	permit interface-dlci
permit bandwidth	permit pvc	permit no motd-banner	permit lmi-type ansi
permit clock	permit load-interval	permit no password	deny tag-switching
deny erase	permit access-list	permit no speed	permit fair-queue
deny write erase	permit protocol	permit no telnet	permit no fair-queue
deny debug all	permit width	permit no timeout	permit dsip
permit reload	permit atm	permit no width	permit undebug all
permit ping	permit map-group	permit no x25	deny ip cef
permit traceroute	permit x25	permit no access-list	deny no ip cef
permit shutdown	permit motd-banner	permit no pvc	deny clear ip cef
permit no shutdown	permit mtu	permit no atm	permit no modem
permit cd	permit no interface	permit no protocol	permit modem
permit dir	permit no full-duplex	permit no width	permit no radius-server
permit loopback	permit no ip	permit no map-group	permit half-duplex
permit send	permit no loopback	permit no mtu	permit full-duplex
permit copy	permit no description	permit no load-interval	permit no peer
permit encapsulation	permit no clock	permit session-timeout	permit no session-limit
permit ppp	permit no bandwidth	permit no session-timeout	permit radius-server
permit async	permit no encapsulation	permit exec-timeout	permit no hold-queue
permit group-range	permit no ppp	permit no exec-timeout	permit session-limit
permit hold-queue	permit no async	permit autoselect	
permit peer	permit no group-range	permit no autoselect	

Tabla 3.3.2 Órdenes que puede ejecutar un usuario según su categoría y grupo de trabajo

Por último, para el caso de los usuarios se genera un archivo más que concentra información básica que los identifica. La tabla relaciona el nombre completo del usuario con la dirección de correo electrónico que permitirá contactarlo, su nivel de privilegio y el grupo del que forma parte, así como el estado actual que guarda. Toda esta información se muestra ejemplificada en la tabla 3.3.3.

No. Consecutivo	1	2	3
Usuario	Antonio Solano Barcenas	Aurelio Matsui Dominguez	Omar Eljure Chavez
e-mail	msolano@mexnet.com.mx	amatsui@ mexnet.com.mx	oeljure@ mexnet.com.mx
Privilegio	acceso usuario	acceso usuario	acceso usuario
Grupo	U-FAL-CL-Stf	U-FAL-CL-Stf	U-FAL-CL-Stf
posible cuenta	msolano	amatsui	oeljure
Estatus	NO EXISTE	NO EXISTE	NO EXISTE

Tabla 3.3.3 Concentrado de información de usuarios de red

La figura 3.3.1 y 3.3.2 muestra el formato utilizado actualmente para el registro de la información de acceso a los usuarios.

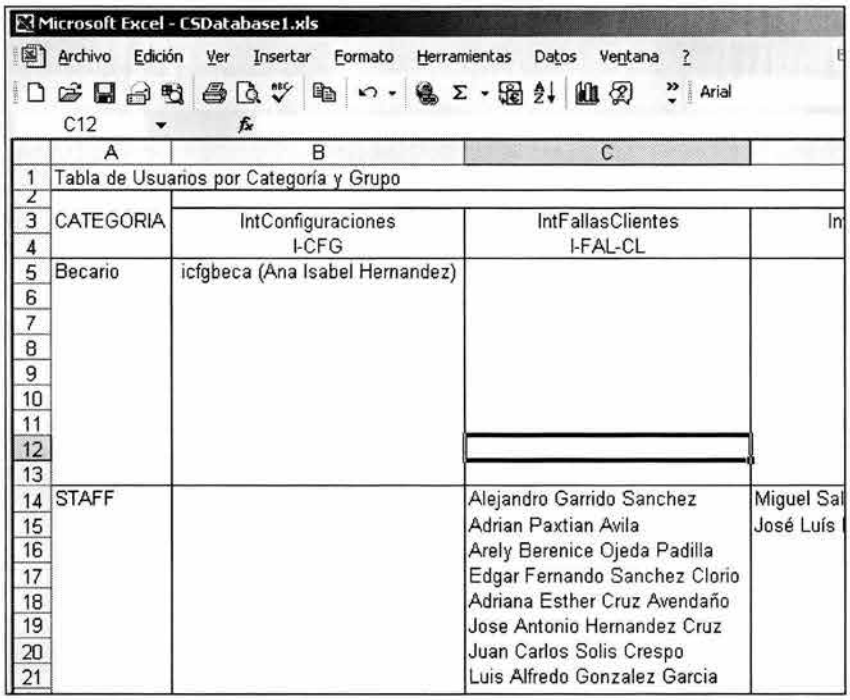
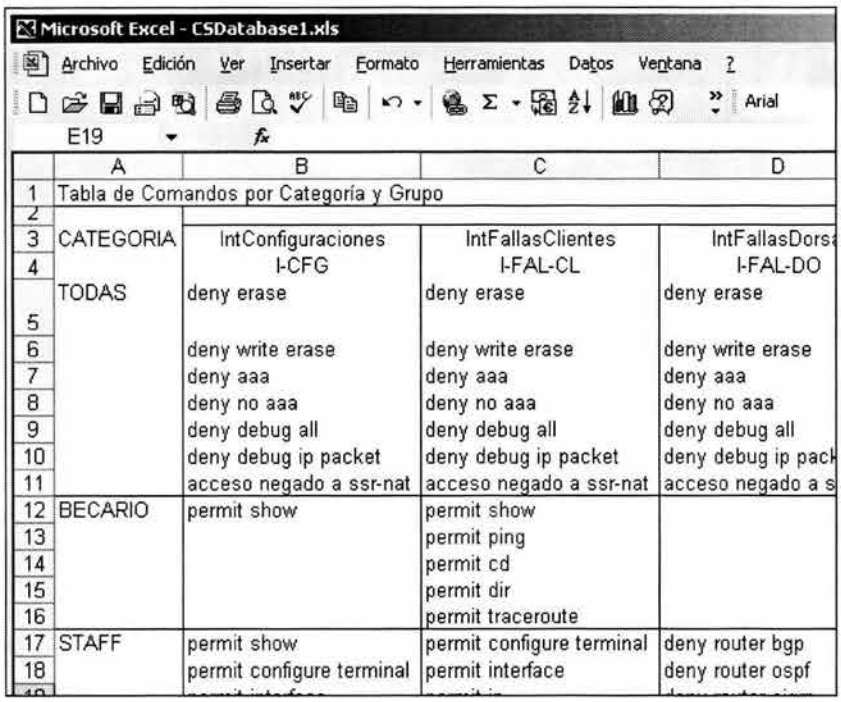


Figura 3.3.1 Administración de usuarios y perfiles actual

En la figura 3.3.1 se observan los grupos de usuarios de acuerdo al área y nivel de jerarquía dentro de la misma. De esta forma se administran los perfiles. Dentro de cada perfil, se tiene la lista de los usuarios que pertenecen a ese grupo. Para buscar un

usuario en específico, se hacen coincidir las filas y columnas teniendo como datos el área a la que pertenece y el nivel que tiene.



Microsoft Excel - CSDatabase1.xls

Archivo Edición Ver Insertar Formato Herramientas Datos Ventana ?

Arial

E19

	A	B	C	D
1	Tabla de Comandos por Categoría y Grupo			
2				
3	CATEGORIA	IntConfiguraciones	IntFallasClientes	IntFallasDors
4		I-CFG	I-FAL-CL	I-FAL-DO
5	TODAS	deny erase	deny erase	deny erase
6		deny write erase	deny write erase	deny write erase
7		deny aaa	deny aaa	deny aaa
8		deny no aaa	deny no aaa	deny no aaa
9		deny debug all	deny debug all	deny debug all
10		deny debug ip packet	deny debug ip packet	deny debug ip pack
11		acceso negado a ssr-nat	acceso negado a ssr-nat	acceso negado a s
12	BECARIO	permit show	permit show	
13			permit ping	
14			permit cd	
15			permit dir	
16			permit traceroute	
17	STAFF	permit show	permit configure terminal	deny router bgp
18		permit configure terminal	permit interface	deny router ospf

Figura 3.3.2 Administración de perfiles y permisos de usuario

Para ciertas categorías de usuarios se tiene el inventario de los permisos que tienen en la plataforma de equipos correspondiente al que tienen acceso, que generalmente se refiere a los comandos que pueden utilizar. Esta información se maneja de igual forma que la administración de perfiles y usuarios, y se muestra en la figura 3.3.2.

Inventario de equipos de red

Para controlar el inventario de equipos de red, se utiliza el formato de los archivos de texto simple. Inicialmente tenemos que el nombre del archivo contiene la indicación del tipo de dispositivo de que se trata, por ejemplo, TxtSW.txt establece que su contenido es una lista de Switches. En el interior del archivo se tiene una vista similar a la siguiente:

lsw-ags-pedroparga-1.gdl:148.223.108.74:
lsw-ags-pedroparga-2.gdl:200.64.127.141:
lsw-bcn-glzortega-1.her:148.223.107.139:
lsw-bcn-glzortega-2.her:148.223.107.131:
lsw-bcs-lapazbcs-1.her:148.235.63.109:
lsw-bcs-lapazbcs-2.her:200.79.91.152:

Esencialmente, lo que se ve es el nombre del switch (que integra la ubicación física del mismo) seguido por el símbolo ':' , la direción IP que le corresponde internamente y para terminar el símbolo ':' nuevamente.

En el caso de ruteadores y otros dispositivos, el esquema es el mismo; se desea integrar en el nombre del archivo de texto la indicación del tipo de equipo, en el interior, una lista con el nombre de cada dispositivo seguido de su dirección IP. Esto constituye el inventario de equipos tal como se maneja a la fecha. El archivo es editable con cualquier editor de textos común, como el Bloc de notas con el que cuenta Windows, y se puede ver en la figura 3.3.3.

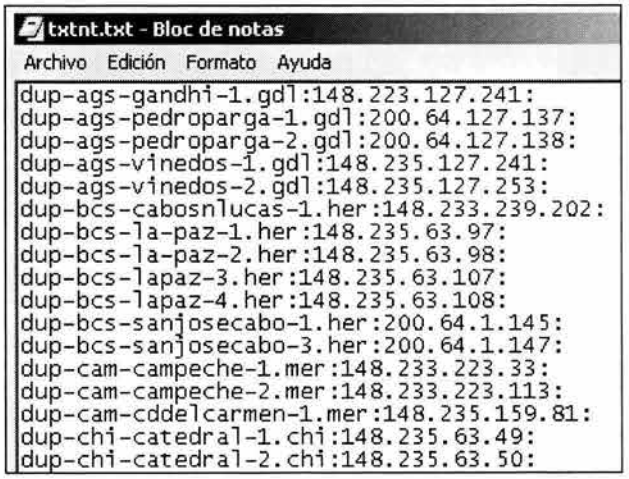


Figura 3.3.3. Ejemplo de archivo de inventario de equipos.

Incidentes de seguridad

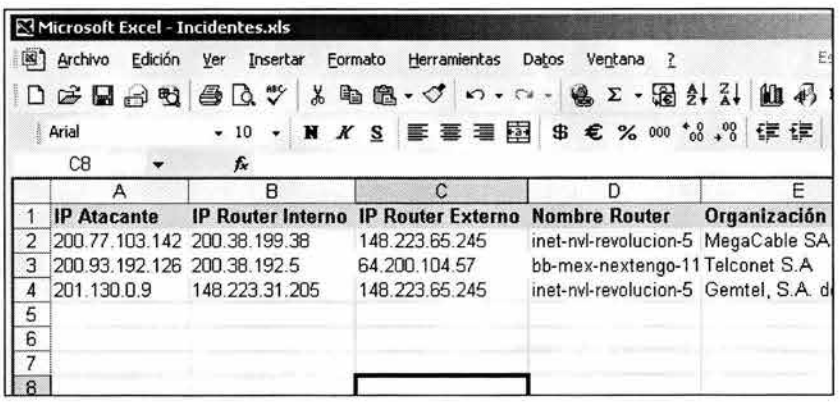
Como se vió en la sección 3.1, al área de seguridad llegan las notificaciones sobre incidentes por vía telefónica o por correo electrónico desde el cliente afectado o desde otro operador de red independiente. Una vez ahí, se obtienen los datos del responsable de la IP origen, para lo que se accede a la información de contacto técnico a través de las páginas de asignación de dominios y direcciones IP mundiales o regionales, en donde se encuentra registrado: país, organización, contacto técnico, teléfono y dirección de correo electrónico. A esta información se le anexa la resultante de hacer una traza a la dirección IP que consiste en el nombre del último ruteador del ISP y el ruteador siguiente a éste y que comunica con la IP fuente del incidente. El resultado de este proceso del incidente de seguridad, produce un archivo de Excel con la estructura mostrada en la tabla 3.3.4.

IP Atacante	200.77.103.142	200.93.192.126	201.130.0.9
IP Ruteador Interno	200.38.199.38	200.38.192.5	148.223.31.205
IP Ruteador Externo	148.223.65.245	64.200.104.57	148.223.65.245
Nombre Ruteador	Inet-nvl-revoluciona-9	Inet-mex-nextengo-13	Inet-nvl-revolucion-9
Organización	SuperCable SA de CV	Telconet S.A	GeneraTel, S.A. de C.V.
Tipo Incidente	SPAM	SCAN	VIRUS
Fecha/Hora	10-06-03 11:19	13-06-03 01:23	15-06-03 09:28
Contacto	NIC TECH	Servio Limón	Arturo Cruzada Torrejo
Teléfono	+52 33 37500029		222 2666060
Email	nictech@supercable.com	slimon@teconecta.net	atorres@generatel.com
Observaciones			

Tabla 3.3.4 Estructura de archivo en Excel para registro de incidentes de seguridad

Los elementos de la columna izquierda de la tabla 3.3.1, son los encabezados de la tabla en Excel y las tres columnas siguientes son ejemplos de valores a registrar en la misma.

En la figura 3.3.2, se presenta el formato de Microsoft Excel utilizado, en el cual cada nuevo registro de incidente de seguridad se va agregando a un nuevo renglón de la hoja, y una vez que un incidente se resuelve se cierra el caso marcándolo con un color diferente al predeterminado.



	A	B	C	D	E
1	**IP Atacante**	**IP Router Interno**	**IP Router Externo**	**Nombre Router**	**Organización**
2	200.77.103.142	200.38.199.38	148.223.65.245	inet-nvl-revolucion-5	MegaCable SA
3	200.93.192.126	200.38.192.5	64.200.104.57	bb-mex-nextengo-11	Telconet S.A
4	201.130.0.9	148.223.31.205	148.223.65.245	inet-nvl-revolucion-5	Gemtel, S.A. d
5					
6					
7					
8					

Figura 3.3.2 Formato utilizado para el registro de incidentes de seguridad

De la tabla, sólo el dato correspondiente a 'tipo de incidente', proviene de un catálogo existente que se ha definido de forma conveniente.

Como puede verse, la forma de registro de inventario de incidentes, usuarios y equipo se centra principalmente en la elaboración de archivos independientes en formato de excel y de texto simple que se deben organizar manualmente en carpetas y controlar de manera tal que se mantenga un seguimiento de cada tipo de inventario. Este proceso como puede verse, puede ser mejorado con el uso de una buena base de datos que integre la información (centralización) a la vez que permita organizarla y recuperarla de manera rápida y sencilla, reduciendo problemas de administración, tiempos y errores de captura, así como para realizar las notificaciones correspondientes.

3.4 IDENTIFICACIÓN DEL PROBLEMA

El aspecto principal a cubrir con el nuevo sistema de administración de inventarios, es la automatización de los pasos y procesos que se llevan a cabo para tener la información de los usuarios y equipos de la red, así como la captura de los incidentes de seguridad en un sistema que permita, la consulta de cualquier caso desde cualquiera de las terminales de operación de los administradores de seguridad, así como evitar el tiempo de captura excesiva cuando una dirección IP tiene reincidencia, mediante la consulta automática de los datos que ya se capturaron con anterioridad.

Administración de usuarios

En la administración de los inventarios de usuarios se cuenta actualmente con varios archivos de acuerdo a la plataforma de que se trata, buscándose la centralización de la información en un medio de almacenamiento físico y lógico seguro, como lo es un servidor y una base de datos robusta.

Dentro de esta base de datos centralizada, se contará con una clasificación de plataformas de usuarios mediante un catálogo de categorías y en las cuales se indicará el tipo de que se trata, por ejemplo, usuarios de la página de reportes, usuarios de la plataforma TACACS+, usuarios de la plataforma RADIUS, etc. Y de acuerdo a esta clasificación, cada categoría podrá contener un grupo de tablas que identificará a sus grupos, usuarios y permisos, en caso de que exista una administración de ellos.

Para dar de alta un nuevo usuario, el administrador de seguridad solamente tendrá que capturar todos sus datos. Se busca facilitar la generación de las contraseñas, mediante un algoritmo que permita incluir en una cadena aleatoria de ocho o diez caracteres, letras, números y algunos caracteres especiales.

En la figura 3.1.1, se observa el proceso actual para el alta de nuevas cuentas de usuario o bien la modificación de alguna existente. El proceso se genera de manera

manual, desde la recepción de la solicitud, hasta el envío de la notificación al usuario donde se le indica su información de acceso. Actualmente no se lleva registro alguno de la fecha en la que una cuenta de usuario se da de alta o se modifica, lo cual resultaría importante para casos de seguimiento de casos, y que permita al administrador saber con certeza cuando se generó o modifico alguna.

- La recepción de la solicitud, se seguirá haciendo como hasta ahora, mediante correo electrónico, solamente se tiene que indicar en ella, el nombre de la persona a la que la cuenta pertenecerá, el área donde labora y el correo electrónico a donde la información de acceso será enviada.

- La identificación de la plataforma, se hará con los datos contenidos en el correo de solicitud. El sistema permitirá la selección de la plataforma donde se creará la cuenta de forma similar al explorador de Windows, en donde el administrador irá explorando el árbol de elementos de la Administración de Seguridad, hasta llegar al nodo indicado, en el cual seleccionará la opción Nuevo, para disparar el cuadro de diálogo que permita la captura de la información.

- La generación de la contraseña, será automática con solo presionar un botón. La contraseña generada cumplirá con el requerimiento particular para su formato, no teniendo que editarla nuevamente para cambiar algún carácter que no cumpla con ello. Adicionalmente, esta generación permitirá obtener de forma aleatoria la llave de encriptación para su almacenamiento en la base de datos, la cual cambiará de guardarse en formato de texto claro, es decir, sin ningún tipo de encriptación, a la manera encriptada, permitiendo solo a quien conoce la llave y el algoritmo de encriptación, la obtención de la contraseña.

- El registro o modificación de la cuenta, que se hace actualmente en un archivo de excel, será almacenada en una tabla de SQL Server, dependiendo de la categoría de usuarios modificada, y con toda la información especificada en la captura. La contraseña estará encriptada, y la fecha de actualización será generada

automáticamente de acuerdo a la fecha del sistema, el administrador no interviene en este aspecto.

- Notificación. Para evitar errores en la generación de una notificación de cuenta activada, por ejemplo en la transcripción de las contraseñas de acceso, o en el nombre de usuario, se utilizará el concepto de notificación automática, que constará de una plantilla de mensaje, en la cual será incluido el nombre de usuario, su o sus contraseñas y una notificación de advertencia para el uso indebido de la misma. Con anterioridad esta notificación se tenía que escribir nuevamente para cada usuario creado o modificado, teniendo que transcribir los datos de acceso al mensaje de correo, generando errores con frecuencia. Este esquema automático permitirá con solo presionar un botón en la aplicación, la generación y envío de la notificación a la dirección de correo electrónico especificada en la captura de datos y tomando la información de acceso de la tabla de usuarios.

- El uso de notificaciones automáticas se extiende a los casos en que algún usuario olvidaba o perdía su(s) contraseña(s) y en las que se debía generar nuevamente la notificación para hacerle saber sus contraseñas. Ahora solo se tendrá que buscar al usuario y una vez encontrado, elegir la opción de notificación para generarla y enviarla automáticamente.

- El módulo contará con la opción de baja de usuarios, la cual se realizará haciendo la búsqueda del mismo y eliminándolo del catálogo de usuarios.

Administración de perfiles

Así como para cada categoría se tienen sus usuarios específicos, también contará con los perfiles. Estos perfiles permiten organizar a los usuarios de acuerdo a su área y funciones. Todos los usuarios contenidos en un mismo grupo o perfil tendrán

exactamente los mismos permisos y si cambia alguno al grupo, cambiará a todos los usuarios.

En la figura 3.1.2 se muestra el proceso actual, en donde se presentarán las siguientes mejoras en el proceso de administración de perfiles.

- La solicitud será recibida por correo electrónico o telefónicamente.
- La identificación de la plataforma se realiza también mediante la exploración en la interfaz principal del sistema.
- Permite la centralización del inventario de grupos y permisos a usuarios.
- Permite la exportación de la información a un archivo que podrá ser analizado por Excel, en caso de requerirse algún reporte de permisos almacenados. Este archivo es generado internamente por el sistema al darle la indicación y no es necesaria ningún tipo de intervención manual.

Administración de equipos

El proceso actual de administración del inventario de equipos se muestra en la figura 3.1.3 en donde básicamente se pretende centralizar y asegurar toda la información existente en múltiples archivos de texto plano, y que no ofrecen seguridad alguna en cuanto a su contenido.

De acuerdo al procedimiento de integración de equipos al inventario, se tienen las siguientes ventajas que ofrecerá el sistema sobre el proceso actual.

- La solicitud de integración se recibe de igual manera, en un mensaje de correo electrónico, indicando el nombre del equipo a dar de alta y su dirección IP.

- Para integrar un equipo, éste debe pertenecer a una plataforma específica la cual deberá ser creada antes de comenzar a integrarlos, es decir, no existirá ningún equipo que no cuente con una plataforma asociada. Esta validación es importante porque nos permitirá reducir al mínimo los errores derivados de ello.

- Se tendrá un control de duplicidad, y por tanto del inventario numérico real de los equipos. En la actualidad, no existe ningún tipo de validación cuando se integra alguno, es decir, si no se tiene el debido cuidado, puede existir un equipo dos veces en el mismo archivo, o bien estar dado de alta en archivos diferentes, en caso de confusión con la plataforma. En el caso del sistema, este riesgo se elimina, una vez que un equipo sea dado de alta, no será posible darlo de alta otra vez, inclusive si la plataforma donde se intenta hacerlo es otra.

- Se elimina el uso de muchos archivos de texto, y en cambio se almacenan en una sola base de datos, que permitirá clasificarlos por un campo dentro de la misma.

- La generación de contraseñas manualmente, como es manejado en la actualidad, se cambia por un esquema similar al que operará con las contraseñas de los usuarios. Se generarán con solo elegir la opción, y será generada al mismo tiempo y de forma aleatoria las llaves de encriptación, permitiendo que solo con ellas se conozca la o las contraseñas. Con lo anterior se elimina la vulnerabilidad con la que cuentan los archivos de texto, la cual no ofrece ningún tipo de seguridad para el almacenamiento de contraseñas, y siendo un archivo de texto, cualquier intruso que ingresara al equipo donde los archivos se encuentran, podría verlos con solo abrirlos en bloc de notas.

- Se ofrecerá la opción de compatibilidad con los archivos de texto para uso exclusivo del personal de seguridad, y que para fines de reporte, permitirá la exportación de la información de una plataforma específica a un archivo de texto, con el formato que se ha venido manejando hasta el tiempo actual. La ventaja es

que la generación de este archivo se hará de manera local, es decir, únicamente en el equipo cliente que solicite esa exportación y en ningún caso será generada en el servidor, por lo que cada vez que se ejecute esa opción se tendrá que acceder forzosamente al servidor, con los permisos necesarios para la base de datos y hacer directamente la consulta a través del sistema.

Administración de incidentes de seguridad

El proceso actual que se realiza para la atención a los incidentes de seguridad que se presentan en la red del ISP, es mostrado en la figura 3.1.4.

Las ventajas en este proceso se verán reflejadas principalmente en el registro de los incidentes, ya que minimiza el tiempo de captura, y en las notificaciones. Las ventajas que ofrece el sistema en este aspecto de la operación del Departamento de Seguridad son las siguientes:

- Permitirá la captura de un incidente en una sola base de datos y no en las hojas de Excel actuales que tienen que ser segmentadas en varios archivos debido al volumen de información que pueden manejar. En este caso toda la información de incidentes es ingresada en una sola tabla de la base de datos.

- El tipo de incidente es manejado en base a un catálogo establecido de acuerdo a los casos presentados, que serán seleccionados de un control con opción múltiple y no escritos manualmente. Esto evita problemas debidos a la captura manual de este dato, ya que, por ejemplo, para un tipo de incidente de Rastreo de Puertos, un administrador de seguridad lo podría escribir como 'Escaneo de puertos', otro administrador como 'Scaneo de puertos' o 'Port Scan', siendo que es el mismo tipo de incidente. Al momento de hacer la clasificación mensual, había que contemplar los casos como uno mismo, aumentando el tiempo de análisis. Al ofrecer una opción de selección de tipo de incidente, solo podrán seleccionar el correcto, ya que no permitirá que los administradores lo escriban

- La captura de la fecha del incidente, es validada, no permitiendo que se escriban fechas del futuro o bien con formato incorrecto.

- La captura del correo electrónico del contacto técnico de la organización responsable de la dirección IP que genera el incidente, es muy importante ya que a través de ella, será posible la notificación del mismo al contacto.

- La notificación vía correo electrónico que se realiza actualmente al responsable de la dirección IP, se hace manualmente, es decir, una vez que se captura la información correspondiente, se escribe un correo electrónico en cualquier cliente de correo, como puede ser Microsoft Outlook, redactando en español e inglés el problema detectado con la dirección IP en cuestión, e indicando la fecha y hora de la detección o reporte, así como el tipo de incidente presentado. Si se trata de más de una incidencia, se cuentan los renglones que pertenecen a la misma dirección y se especifica cada uno.

  Con el sistema se eliminará este proceso, que en la mayoría de los casos, es algo tardado (se tiene que hacer para cada incidente), y que puede llegar a omitir o enviar información con error respecto a la capturada.

  Una vez que se registre el incidente en la base de datos, se creará un registro en la tabla correspondiente. De acuerdo a un campo de control en el registro, el sistema puede identificar los incidentes de los cuales no se ha generado notificación. Adicionalmente se integrará un módulo de notificación de incidentes de seguridad, que se tratará de un proceso en el cual se revisarán todos los registros capturados de los cuales no se hayan generado notificaciones, tomará cada uno de los registros pertenecientes a una dirección IP específica, y generará la plantilla de notificación que contendrá un texto que informe al responsable de la causa del mensaje de correo, e incluyendo los detalles de cada incidencia perteneciente a la IP en cuestión, tales como, la fecha, hora y tipo de incidente.

Este proceso se hará para todas las direcciones IP que se encuentren en la tabla de incidentes en las que su campo de control indique que no se han enviado notificaciones. Una vez que se construya esta plantilla, se enviará el mensaje al responsable.

El proceso anterior permitirá que una vez que se genera una notificación de un incidente de seguridad, se marquen las direcciones IP involucradas como notificadas, y en caso de reincidencia y casos en que se capturen nuevos incidentes de la misma IP, se genere una nueva notificación, sin repetir en ella las ocasiones anteriores.

- Mediante una interacción con el responsable de las direcciones IP con incidentes, se van teniendo avances en la solución de ellos, que pueden tratarse por correo electrónico o bien por teléfono. Estos avances se irán documentando en un campo llamado observaciones y en el cual se registren. Cuando se llegue a la solución del incidente, y no se reciban más reportes de una misma IP, se procederá a cerrar el caso. Para este proceso se tendrá otro campo de control en la tabla de incidentes, donde se indicará cuando el caso ha sido resuelto y cerrado, y para efectos de reportes, se contabilizarán como resueltos el numero de incidentes presentados para una IP, por ejemplo, si de la dirección IP 192.168.100.1 se reciben 5 reportes de incidentes de seguridad, cuando se resuelva el caso, se cerrarán un total de 5 reportes.

Notificaciones de Seguridad

Las notificaciones de seguridad se diferencian de los dos casos anteriores de notificaciones, en que éstas últimas pueden ser enviadas en consecuencia a la aparición de un evento de seguridad, interno o externo a la empresa.

En el caso de eventos internos, podría tratarse de algún incidente que afecte la operación de la red y que de alguna manera tenga que ser conocido por todos los integrantes de la empresa, por ejemplo, la presencia de algún virus en la red interna.

En el caso de eventos externos, podría tratarse de la aparición de algún virus que no forzosamente haya afectado a algún equipo interno, pero que su aparición en la red mundial, deba ser comentada o informada para evitar caer en un problema posterior si se presentara internamente. La aparición de nuevos parches a los sistemas que por su criticidad tenga que ser aplicada a los sistemas de la empresa, es importante contemplarlos en estas notificaciones.

La ventaja que ofrecerá el sistema respecto a este punto, es la rapidez con la que puede hacerse envío de una notificación, ya que tendrá que escribirse una sola vez, y una vez escrita guardarla en la base de datos para futuras referencias, y al momento de enviarlas, simplemente se indicará la plataforma de usuarios de la red a la que será enviada y se seleccionará la opción de enviar, sin necesidad de utilizar un cliente de correo en donde tenga que escribirse dirección por dirección de correo para hacer el envío.

Reportes

Los reportes son una parte importante del sistema, ya que en la actualidad, para generarlos, es necesario realizar un conteo minucioso de las actividades que se realizan en el departamento, mediante la consulta de varios archivos de texto o de Excel, el conteo manual y el formato del reporte, llevándose un tiempo largo en su obtención y que en ocasiones se preste a la facilidad de tener errores.

La finalidad de los reportes es pasar todo ese proceso de obtención de datos, contabilización y formateo a las terminales de operación y quitarlo de las manos del personal, simplemente solicitando la información requerida, y después de un

procesamiento interno del equipo, obtener una salida ya con el formato y requerimientos necesarios.

Al mismo tiempo, al existir otras áreas que interactúan con el Departamento de Seguridad y que de alguna forma pueden requerir de esta información en cualquier momento, puedan hacerlo mediante un servidor WEB, que genere los reportes rápidamente y se eviten tiempos de espera donde van involucrados el tiempo de la solicitud, el procesamiento humano y la respuesta final.

Ventajas generales sobre la operación del Departamento de Seguridad

Toda la información que será manipulada a través del sistema podrá ser guardada en un solo servidor seguro que contenga la base de datos global, y la cual será accedida únicamente por el personal de seguridad.

El administrador de seguridad contará con un elemento importante para su trabajo, en donde sabrá que la información almacenada no tendrá problemas de seguridad, será única y siempre que la consulte, la obtendrá en un tiempo mucho menor al que implique abrir varias aplicaciones y buscar en varios archivos.

Existirá siempre la opción de búsqueda para las actividades realizadas en los módulos principales del sistema, que permitirán al operador acceder a la información en el lugar exacto donde esta se encuentra, en unos cuantos segundos.

Ofrecerá la compatibilidad con los formatos que se manejan actualmente, sin poner en riesgo la información, ya que, como se mencionó anteriormente, será procesada y generada en las terminales, no en el servidor, y a través del sistema únicamente.

Todo esto en un ambiente amigable y similar al que Microsoft Windows ofrece.

3.5 OPCIONES DE SOLUCIÓN Y ELECCIÓN DE LA ÓPTIMA

Para la solución del problema, se determina la implementación de una base de datos cliente-servidor, para lo cual se proponen como opciones Delphi, PowerBuilder y Visual Basic para el Front-End y MySQL, Oracle y SQL Server para el Back-End. De estas herramientas se realiza una comparación para la elección de la solución.

Front-End

Una base de datos cliente/servidor es una combinación de hardware y software, cuya utilidad se reduce si no se cuenta con medios de acceso a los datos. A pesar de que los proveedores de bases de datos ofrecen, muchas veces, sus propias herramientas de desarrollo, el verdadero poder de los sistemas cliente/servidor radica en la variedad de aplicaciones cliente y software de desarrollo - también llamados Front-Ends -, disponibles por parte de terceros.

Las herramientas de desarrollo de aplicaciones son usadas principalmente por los programadores y están diseñadas para facilitar el proceso de creación de aplicaciones Front-End personalizadas.

De los productos Front-End disponibles, se describen algunos de los productos más conocidos: Delphi, PowerBuilder y Visual Basic, en orden alfabético.

Las herramientas mencionadas cumplen los siguientes criterios:

- Son herramientas de desarrollo visual.
- Están orientadas a ambientes cliente/servidor.
- Corren bajo la plataforma Windows.
- Permiten la conexión a distintos tipos de servidores de datos.

Visual Basic junto con Delphi, son herramientas simples para desarrollo, ya que carecen de facilidades para la programación de proyectos a nivel corporativo, por lo que se les denomina "low-client". PowerBuilder en una herramienta que puede desarrollar y ejecutar proyectos en diversas plataformas sin estar restringida a la PC por lo que se le denomina "multiplataforma".

¿Cómo trabajan los Front-Ends?

Las aplicaciones cliente se ven y se ejecutan igual que cualquier otra aplicación que el usuario tenga en su PC. Si el software del cliente está diseñado de manera apropiada, el único indicio de que el usuario está usando un Front-End de un servidor remoto de bases de datos, se da cuando tiene que dar tanto su clave como su password para entrar en sesión con dicho servidor.

La secuencia de eventos que ocurren cuando el usuario accede al servidor de bases de datos puede ser generalizada en los siguientes cinco pasos:

- (Cliente). El Front-End formatea la consulta en lenguaje SQL y la envía a través de la red hacia el DBMS.

- (Servidor). El servidor de bases de datos verifica los derechos del usuario sobre los datos que desea consultar (sistema de seguridad).

- (Servidor). Si se cuenta con los derechos correspondientes, el servidor de bases de datos procesa la consulta y regresa los resultados de la misma al Front-End.

- (Cliente). El Front-End recibe la respuesta y la formatea para su presentación al usuario.

- (Cliente). El usuario visualiza y/o manipula los datos y/o reinicia el proceso.

La consulta o query puede ser cualquier acción que el usuario haga sobre la base de datos, como actualizaciones, inserciones, borrados o simples consultas.

La tabla 3.5.1, muestra una comparación técnica de las herramientas de desarrollo que pueden utilizarse para la construcción del sistema.

Producto	Delphi 7.0	Power Builder 8.0	Visual Basic 6.0
Marca	Borland	Sybase	Microsoft
Categoría	Low-End Client	Multiplataforma	Low-End Client
Medio de Distribución	CD-ROM	CD-ROM	CD-ROM
Plataforma de Desarrollo Mínima	Pentium 233 MHz, 32 MB, 75 MB HD	Pentium 133 MHz, 64 MB, 100 MB HD	Pentium 90 MHz, 32MB,80 MB HD
Plataforma de Desarrollo Recomendada	Pentium 233 MHz, 128MB, 160 MB HD	Pentium 233 MHz, 128 MB, 160 MB HD	Pentium 233 MHz, 128MB, 160MB HD
Plataformas de Implantación Soportadas	Windows 98, Windows XP y Windows 2000	Windows 98, Windows NT y Windows 2000 y XP	Windows 95 o posterior, Windows NT y Windows 2000 y XP
Utilerías Extra Incluidas	Ambiente de desarrollo para Linux, Borland Kylix 3 for Delphi.	Ambiente de desarrollo para aplicaciones WEB Muy completa gama de herramientas	Asistentes para aplicaciones. Administrador visual de datos. Programa para añadir ayuda en línea. Diseñador de entorno de datos, de informes. Soporte de Internet.
Bases de Datos Soportadas	Oracle, IBM DB2 e Informix, Microsoft SQL 2000 and SQL Server, MySQL y Borland InterBase.	Oracle	SQL Server, Oracle y soporte de ODBC
Ventajas	Provee el camino de migración a Microsoft .NET. Desarrollo e-business con la libertad de llevar fácilmente soluciones Linux.	Adquirida por Sybase, se puede esperar más integración con él.	Producto pionero y líder en programación general en Windows. Requiere pocos recursos, es rápido y fácil de aprender y usar. Es el más popular del mundo.

Tabla 3.5.1 Comparación de herramientas visuales de desarrollo

Producto	Delphi 7.0	Power Builder 8.0	Visual Basic 6.0
Desventajas	Carece de facilidades para control de versiones o creación de aplicaciones de gran tamaño.	Ambiente de programación jerárquico, un poco diferente al normal.	Únicamente sirve para desarrollar aplicaciones Windows.
Observaciones	Una novedosa herramienta, gran velocidad de ejecución, poderoso lenguaje de programación.	Quizás la más difundida herramienta del mercado, cuenta con un gran soporte de terceros.	Punto de partida y comparación para los demás productos. La versión 6 posee muchas mejoras y es muy competitivo.

Tabla 3.5.1 Comparación de herramientas visuales de desarrollo (continuación)

Conclusiones

Hay que señalar que el número de herramientas cliente/servidor es inmenso, y que todas ellas tienen fortalezas y debilidades. Aun así, hay Front-Ends que por su poder y facilidad de uso sobresalen del resto.

Tras la evaluación, las conclusiones sobre cada herramienta son:

- Delphi: Combina la elaboración de ejecutables de alto desempeño con el primer lenguaje de dos vías, siendo una excelente opción para programadores que no cuenten con un equipo muy poderoso. La tradición de Borland en sus herramientas de desarrollo se observa en todo su esplendor con este producto.

- PowerBuilder: Es muy importante para su futuro lo que Sybase logre hacer de ella, pues si logra integrarla con SQL Server y además mejorar su desempeño, sería la opción obligada para los usuarios de Sybase.

- Visual Basic: Esta herramienta inició el reinado de las herramientas de desarrollo visual, y cuenta con el mayor soporte disponible en la actualidad y posee grandes capacidades en su desempeño.

La decisión de la herramienta de desarrollo a utilizar debe estar subordinada al sistema operativo a usar, la plataforma de hardware con la que se cuenta y el tipo de programadores que desarrollarán las aplicaciones.

Back-End

Resulta muy difícil hacer una comparación entre bases de datos. El desempeño de las bases de datos depende tanto de la experiencia de los desarrolladores que las utilizan y de los administradores como del proveedor de la misma. Se puede utilizar cualquier plataforma RDBMS para desarrollar sistemas estables y eficientes. Sin embargo es posible definir transacciones típicas las cuales pueden ser utilizadas en sistemas de control de inventarios. Después de definir estas transacciones típicas es posible ejecutarlas bajo diferentes sistemas de bases de datos trabajando en diferentes plataformas de hardware y de software.

¿Cómo trabajan los Back-Ends?

Back-End es el proceso encargado de atender a múltiples clientes que hacen peticiones de algún recurso administrado por él; normalmente maneja todas las funciones relacionadas con la mayoría de las reglas del negocio y los recursos de datos. La manera en que trabaja se resume en los siguientes puntos:

- Aceptar los requerimientos de bases de datos que hacen los clientes.

- Procesar requerimientos de bases de datos.

- Formatear datos para trasmitirlos a los clientes.

- Procesar la lógica de la aplicación y realizar validaciones a nivel de bases de datos.

En las tablas 3.5.2 y 3.5.3 se muestran una comparación técnica de los manejadores de bases de datos evaluadas para la parte del Back-End

Producto	SQL Server	Oracle	DB2
Marca	Microsoft	Oracle	IBM
Categoría	Base de datos	Base de datos	Base de datos
Medio de Distribución	CD ROM	CD ROM	CD ROM
Plataforma de Desarrollo Mínima	Procesador Pentium 166 MHz, 32 MB RAM, 95 MB HD	Procesador Pentium 166 MHz, 128 MB RAM, 140 MB HD más 4.5 GB para el Oracle Home Drive (FAT) o 2.8 GB para el Oracle Home Drive (NTFS)	Procesador Pentium 166 MHz, 256 MB RAM, 100 MB HD
Plataformas de Implantación Soportadas	Windows NT Server con Service Pack 5, Windows 2000 Server, XP	Windows NT con Service Pack 5, Windows 2000, XP, Linux kernel 2.4.7 y SUN Solaris 5.8	Windows NT con Service Pack 5, Windows 2000, XP, AIX 4.3.3, 5L, 5.1.0, Linux kernel 2.4.9 y SUN Solaris 7 ó mayor
Ventajas	Más barato, fácil de instalar y administrar	Soporta todas las plataformas conocidas, PL/SQL es más poderoso que el T-SQL	Soporta todas las plataformas conocidas, DB2 SQL es mas poderoso que el T-SQL

Tabla 3.5.2 Comparación de bases de datos

Características	SQL Server 2000	IBM DB2 v8.1	Oracle 9i Database
Longitud del nombre de columnas	128	128	30
Longitud del nombre de índices	128	128	30
Longitud del nombre de tablas	128	128	30
Longitud del nombre de vistas	128	128	30
Tamaño máximo del tipo char()	8000	254	2000
Tamaño máximo del tipo varchar()	8000	32672	4000
Número de columnas máximo por tabla	1024	1012	1000
Longitud máxima por renglón en una tabla	8036	32677	255000
Número máximo de columnas por índice	16	16	32

Tabla 3.5.3 Comparación de límites de bases de datos

Conclusiones

Dentro de estos tres manejadores de bases de datos mencionados es difícil considerar que uno es mejor que los otros. Los tres productos pueden ser utilizados para desarrollar sistemas eficientes y estables.

Resultados del análisis

En base a la información citada en las tablas de comparación técnica de herramientas para Front-End y Back-End, se determinó para la parte de Front-End utilizar Visual Basic 6.0, mientras que para la parte del Back-End utilizar SQL Server 2000 porque ambos son más fáciles de instalar, utilizar y administrar, asimismo tienen la capacidad de integrarse por completo entre ellos y en los servidores y terminales con plataforma Windows; además de ser las herramientas de que dispone la empresa y no contar con presupuesto para adquirir alguna de las otras herramientas evaluadas.

CAPÍTULO IV
DESARROLLO E IMPLEMENTACIÓN DEL SISTEMA

4.1 APLICACIÓN DE LA METODOLOGÍA ELEGIDA

Para entender mejor el ámbito del sistema a desarrollar, mostramos a continuación algunos diagramas que reflejan con mayor claridad tanto el contexto como los procesos internos que el sistema ha de considerar.

4.1.1 Diagrama de contexto

En la figura 4.1.1.1 se ve el diagrama de contexto general de cómo se conectará nuestro sistema con cada una de las áreas que lo rodean.

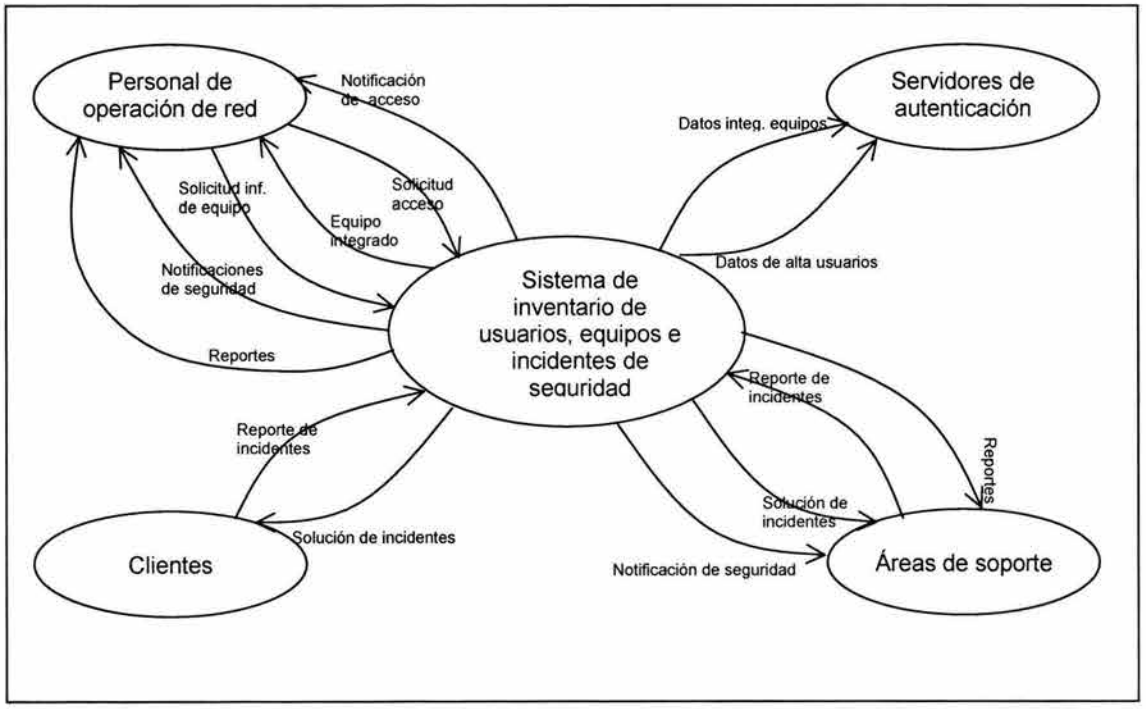


Figura 4.1.1.1 Diagrama de contexto. Nivel I

Diagramas de procesos

En el segundo nivel, podemos ver al sistema conformado por cinco módulos y sus relaciones con los elementos específicos que interactuan con él. En este nivel se aprecia que cada módulo atiende una situación determinada y tiene una comunicación con entes bien determinados.

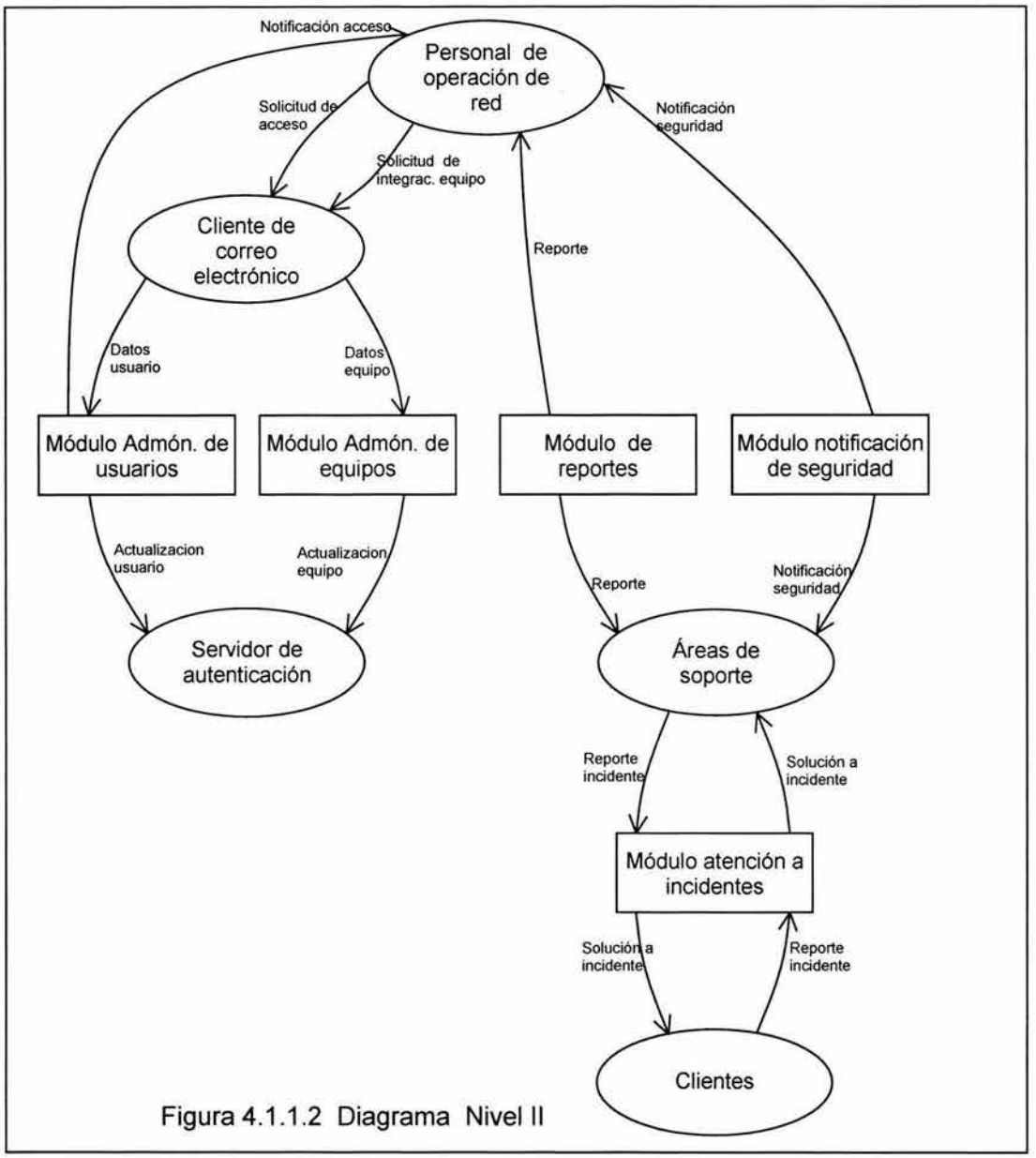


Figura 4.1.1.2 Diagrama Nivel II

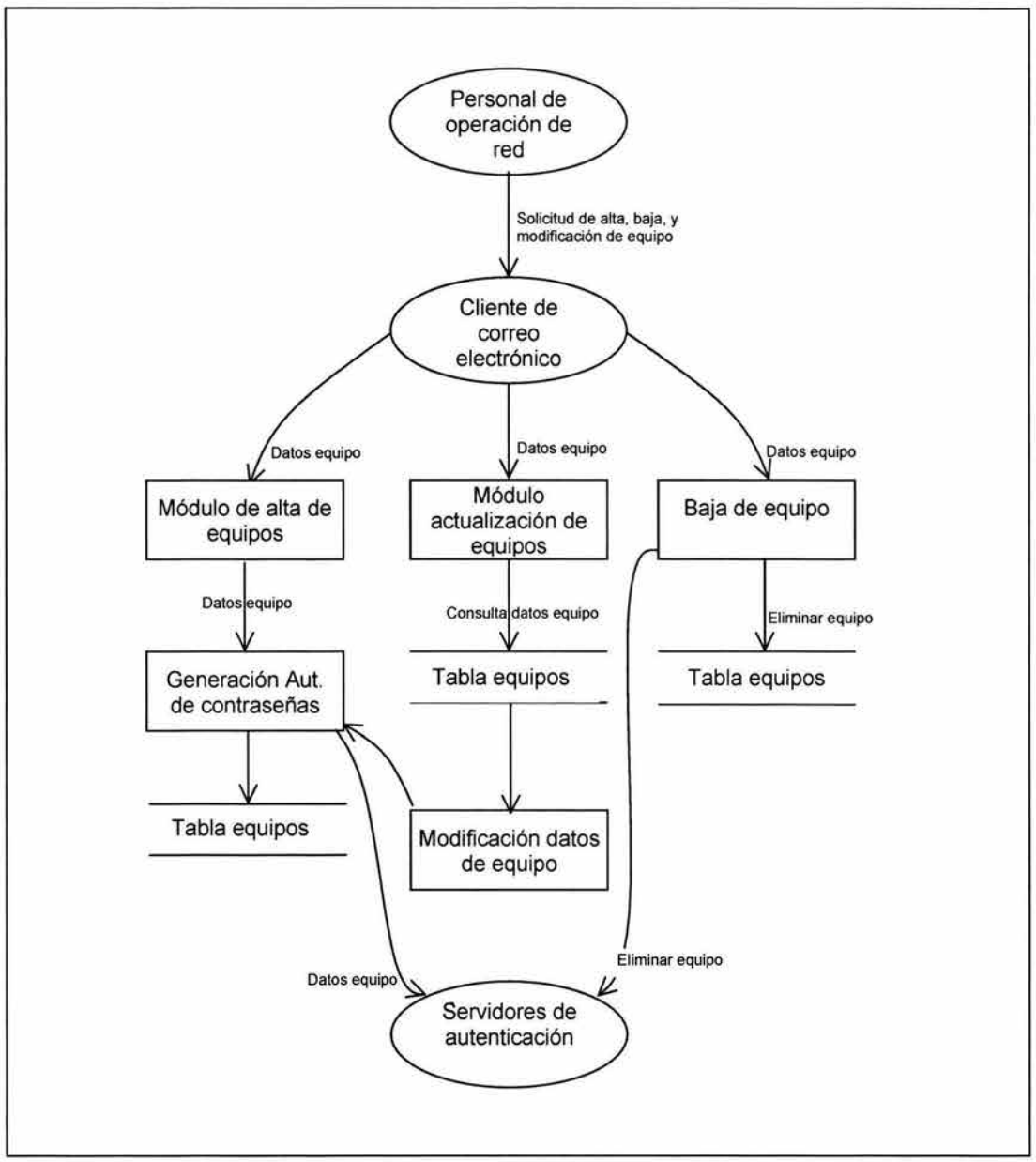


Figura 4.1.1.3 Diagrama de Nivel III. Administración de equipos de red.

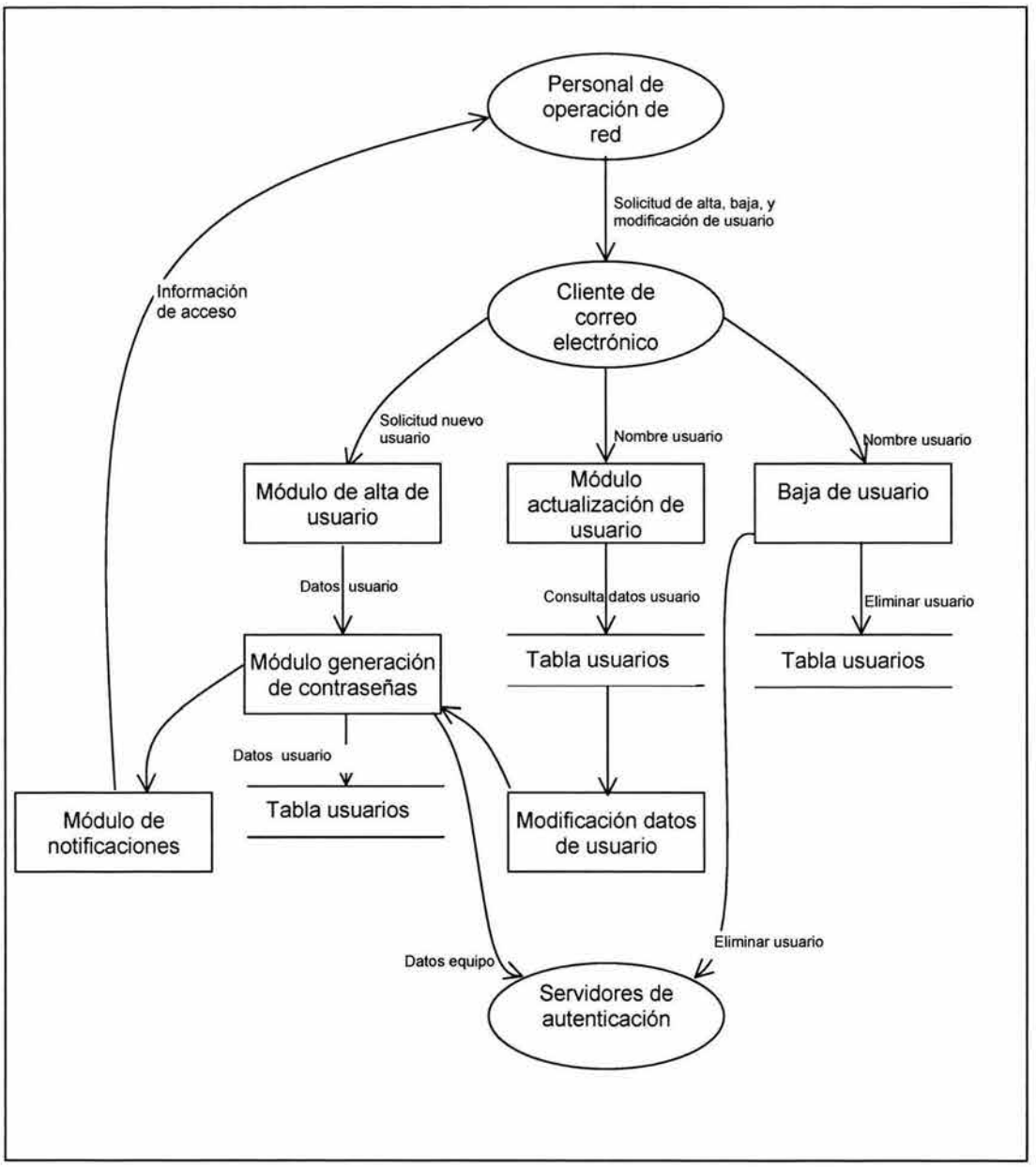


Figura 4.1.1.4 Diagrama de Nivel III. Administración de usuarios de red.

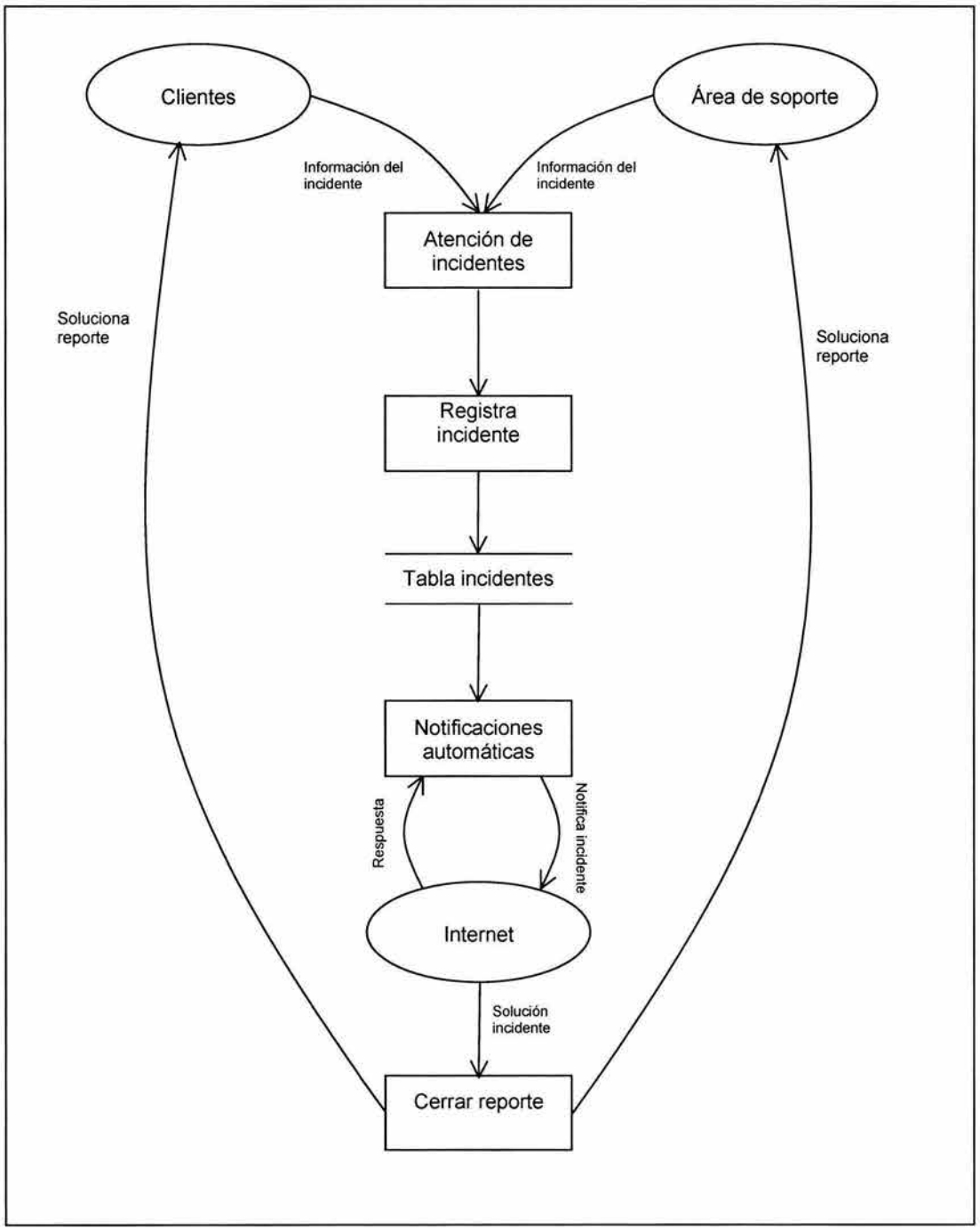


Figura 4.1.1.5 Diagrama de Nivel III. Incidentes de seguridad.

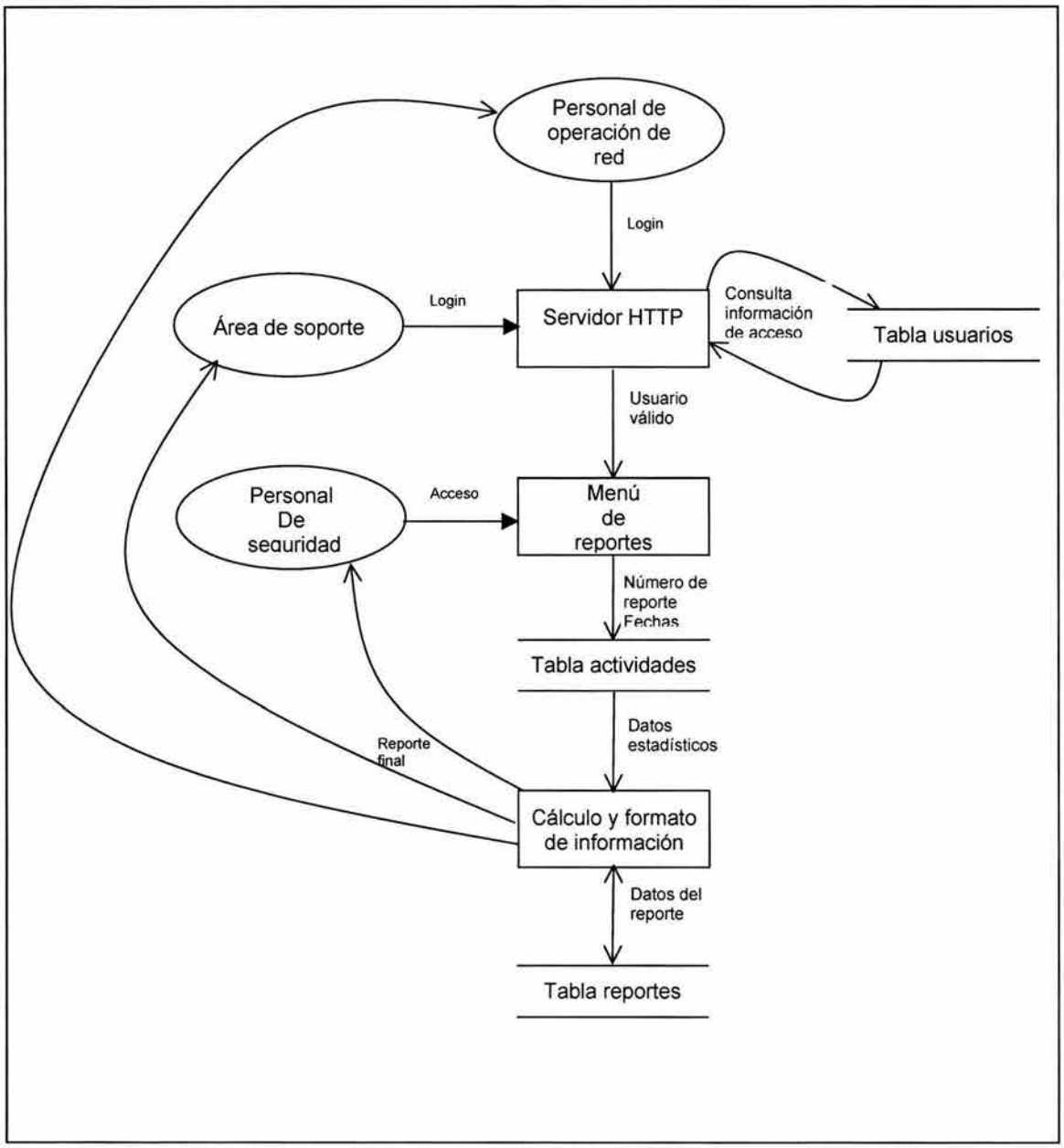


Figura 4.1.1.6 Diagrama de Nivel III. Reportes.

4.1.2 Diagrama de Flujo

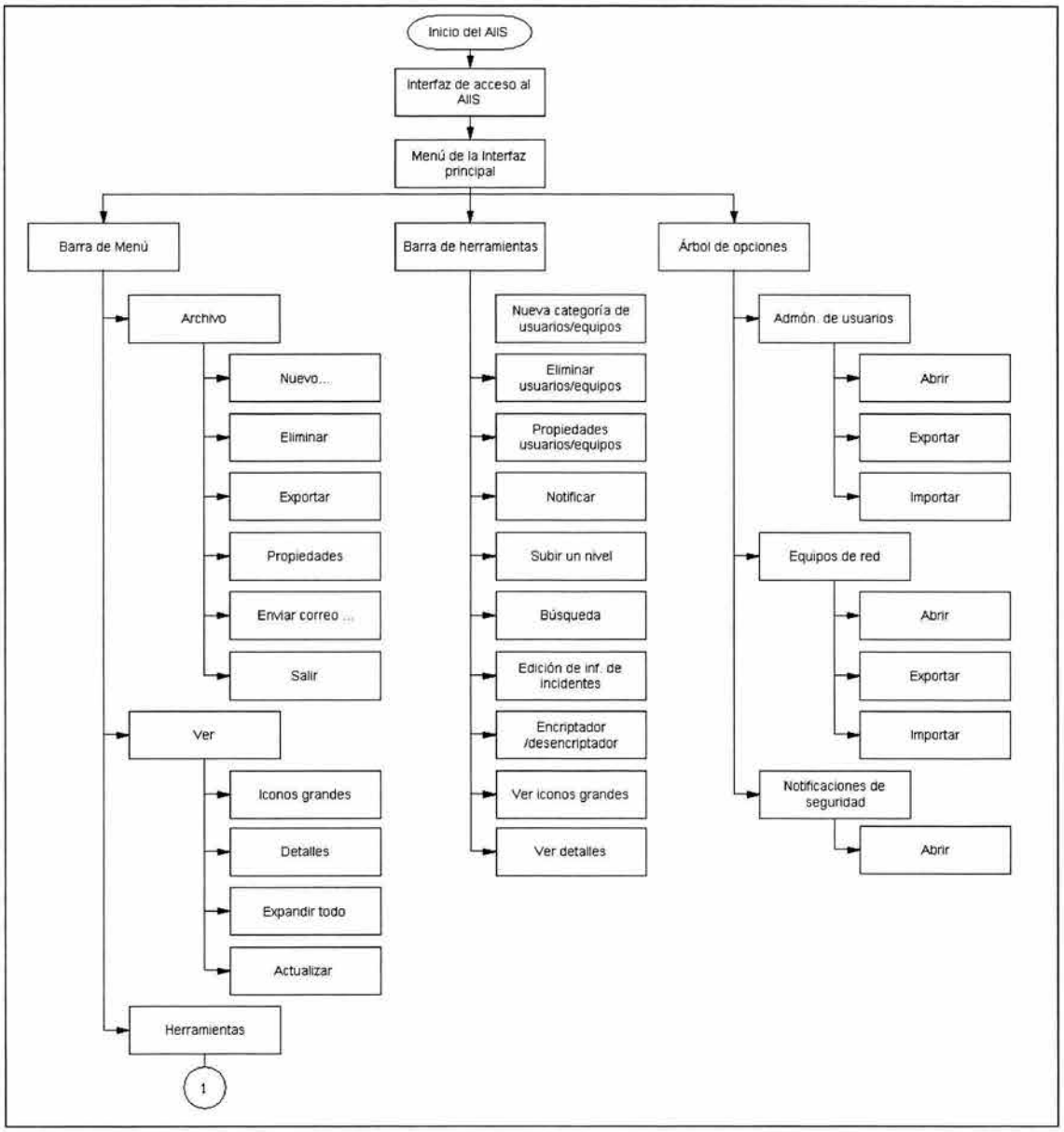
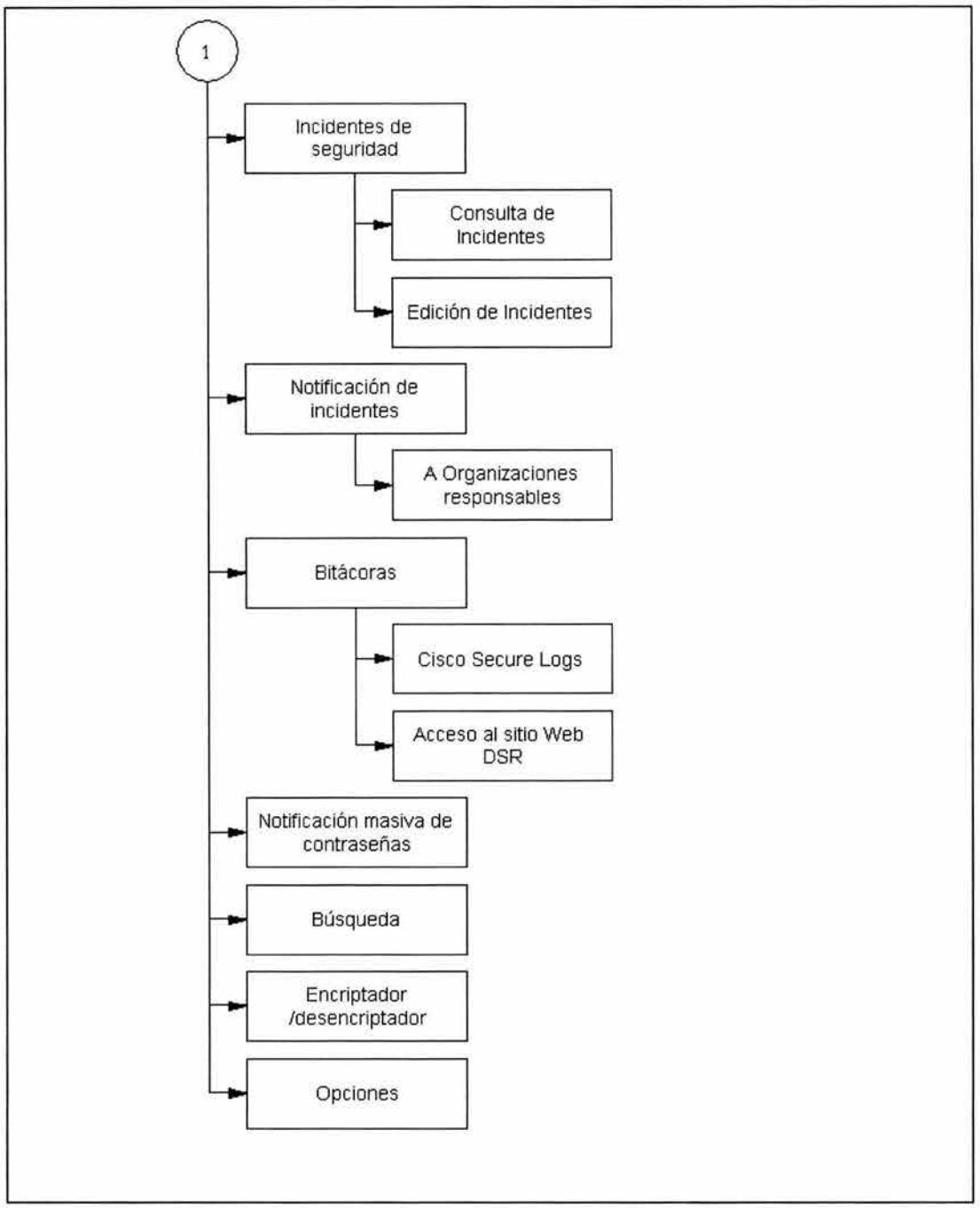


Figura 4.1.2.1 Diagrama de flujo general del sistema



4.1.2.1 Diagrama de flujo general del sistema (Continuación)

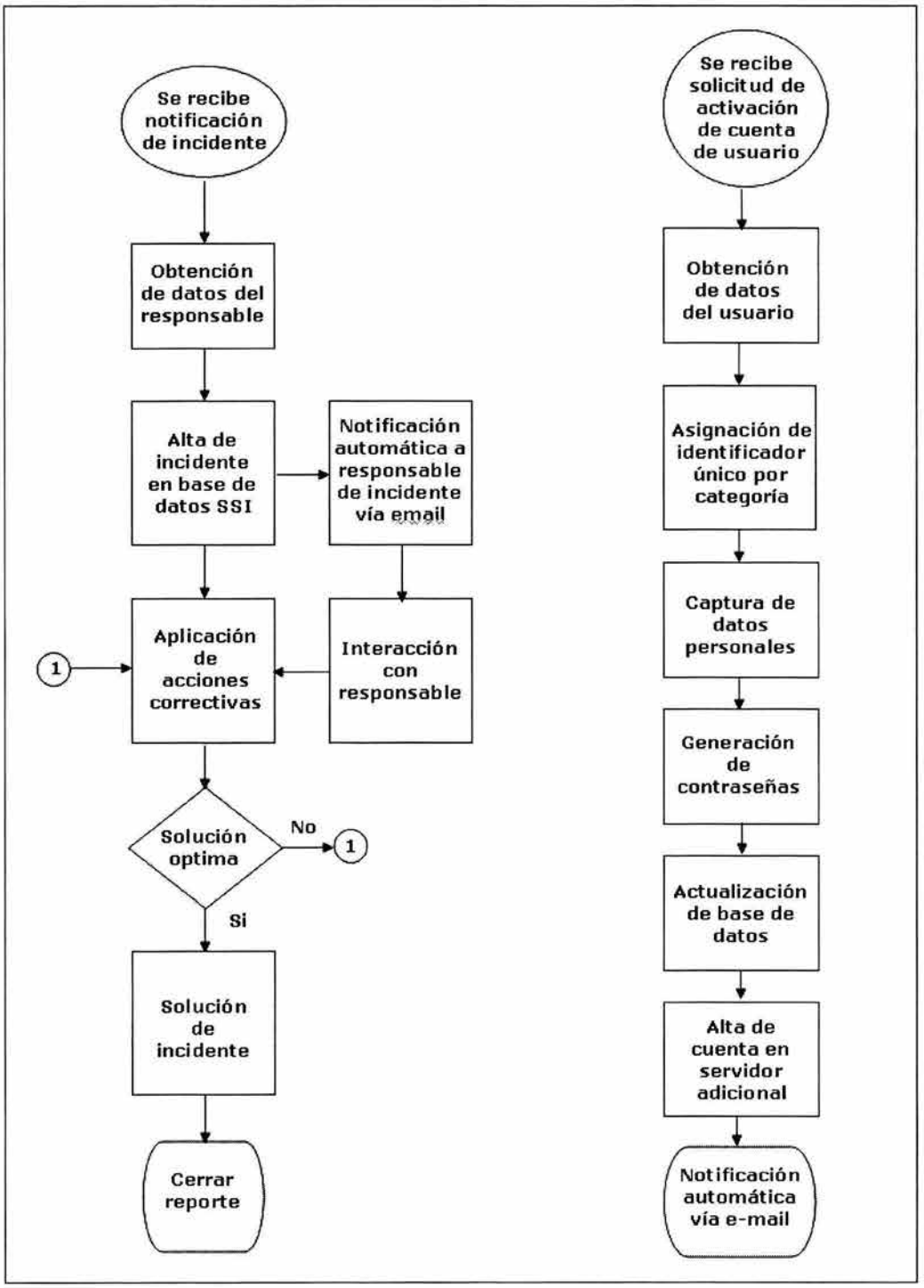


Figura 4.1.2.2 Diagramas de flujo.

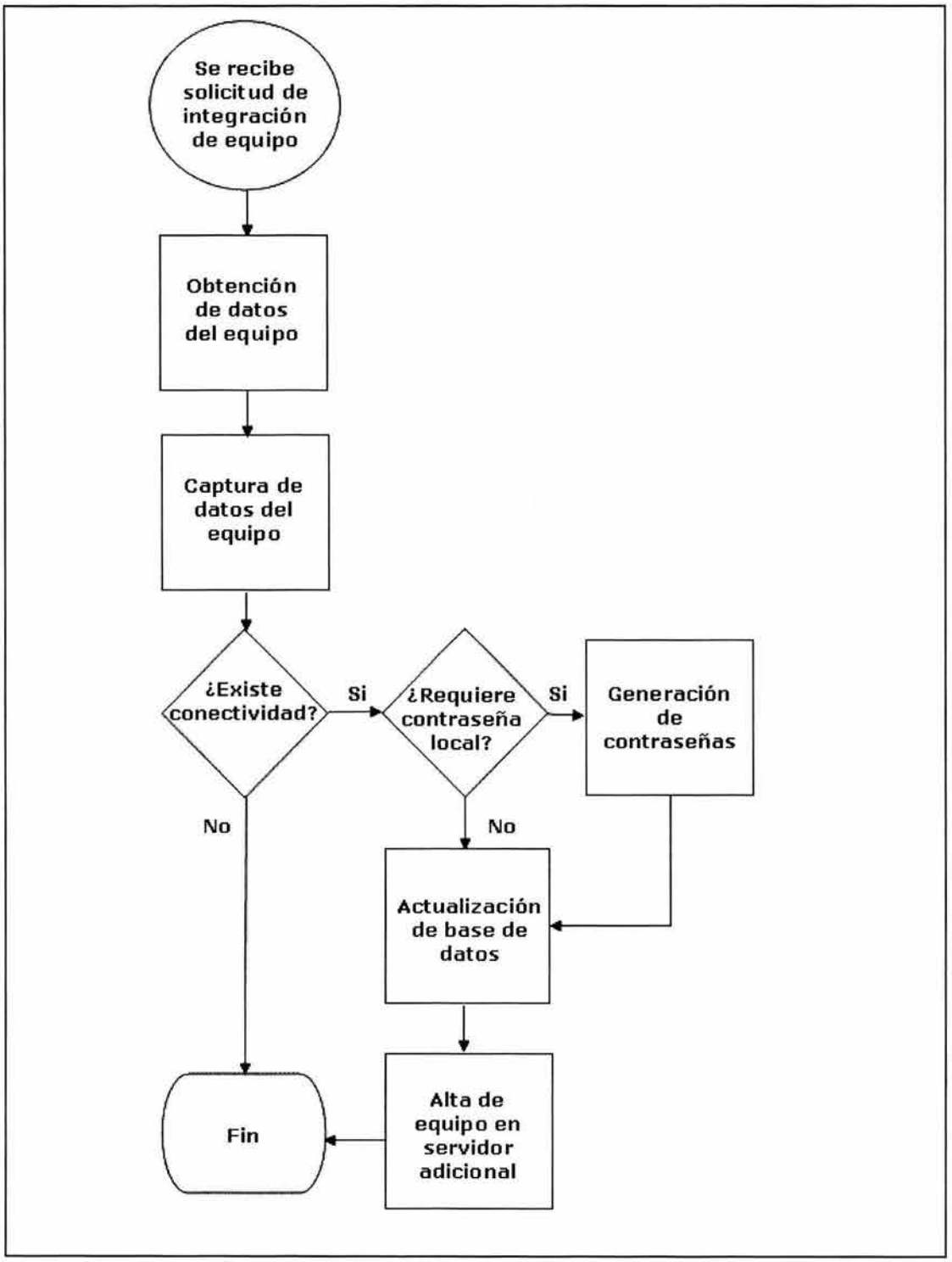


Figura 4.1.2.2 Diagramas de flujo (Continuación)

4.1.3 Diccionario de datos

Administración de usuarios.

Nombre	Acrónimo	Tipo y Longitud	Llave	Descripción	Tabla
Identificador de Categoría de Usuarios	ID_Admin	Varchar(15)	Primaria	Categoría de administración de usuarios de acuerdo a la plataforma a la que tienen acceso	ssradmin_admin_users
Nombre de la categoría	Nombre	Varchar(50)	No	Nombre de la categoría de usuarios	ssradmin_admin._users
Descripción	Descripción	Varchar(50)	No	Descripción de la categoría de usuarios	ssradmin_admin._users
Tabla de usuarios de categoría	Tabla_usr	Varchar(100)	No	Nombre de la tabla que almacenará a los usuarios y sus propiedades de la categoría	ssradmin_admin._users
Tabla de grupos de categoría	Tabla_gpo	Varchar(100)	No	Nombre de la tabla que almacenará a los grupos y sus propiedades de la categoría	ssradmin_admin_users
Tabla de privilegios de categoría	Tabla_cmd	Varchar(100)	No	Nombre de la tabla que almacenará a los privilegios o comandos si aplican en la categoría	ssradmin_admin_users
Identificador de Grupo de usuarios	ID_Grupo	Numérico	Primaria	Identificador único para grupos o perfiles de usuarios existentes en una categoría	ssradmin_<id_admin>_grupos
Identificador de Categoria de usuarios	ID_Admin.	Varchar(15)	Foránea	Identificador de categoría a la que pertenece los grupos o perfiles de usuarios	ssradmin_<id_admin>_grupos

Tabla 4.1.3.1 Diccionario de datos para la administración de usuarios

Nombre	Acrónimo	Tipo y Longitud	Llave	Descripción	Tabla
Nombre del grupo	Nombre	Varchar(50)	No	Nombre del grupo o perfil de usuarios	ssradmin_<id_admin>_grupos
Descripción del grupo	Descripcio n	Varchar(150)	No	Descripción del grupo o perfil de usuarios	ssradmin_<id_admin>_grupos
Nombre de usuario	Username	Varchar(50)	Primaria	Nombre de usuario asignado a la cuenta	ssradmin_<id_admin>_usuarios
Contraseña 1	Passwd1	Varchar(4000)	No	Contraseña número 1 encriptada del usuario	ssradmin_<id_admin>_usuarios
Contraseña 2	Passwd2	Varchar(4000)	No	Contraseña número 2 encriptada del usuario	ssradmin_<id_admin>_usuarios
Llave de encripción	PwdKey	Varchar(3)	No	Llave de encripción de las contraseñas del usuario	ssradmin_<id_admin>_usuarios
Nombre Completo	Nombre	Varchar(255)	No	Nombre completo del usuario	ssradmin_<id_admin>_usuarios
Grupo o perfil	ID_Grupo	Numérico	Foránea	Identificador del Grupo o perfil al que pertenece el usuario	ssradmin_<id_admin>_usuarios
Fecha de última notificación	Ultimo_Cor reo	Fecha	No	Fecha de última notificación automática de contraseñas para un usuario	ssradmin_<id_admin>_usuarios

Tabla 4.1.3.1 Diccionario de datos para la administración de usuarios (Continuación)

Nombre	Acrónimo	Tipo y Longitud	Llave	Descripción	Tabla
Observaciones	Observaciones	Varchar(255)	No	Observaciones o comentarios sobre el usuario	ssradmin_<id_admin>_usuarios
Identificador de grupo o perfil	ID_Grupo	Numerico	Foránea	Identificador del Grupo o perfil al que hace referencia el permiso	ssradmin_<id_admin>_comandos
Comando	Comando	Varchar(255)	No	Comando o instrucción permitida o negada para un grupo	ssradmin_<id_admin>_comandos
Permiso	Permiso	Varchar(10)	No	Permiso o negación de ejecución de un comando	ssradmin_<id_admin>_comandos

Tabla 4.1.3.1 Diccionario de datos para la administración de usuarios (Continuación)

Administración de inventario de equipos de red

En la tabla 4.1.3.2 se presenta el diccionario de datos utilizado en la administración de inventario de equipos de red.

Nombre	Acrónimo	Tipo y Longitud	Llave	Descripción	Tabla
Identificador de plataforma	ID	Varchar(15)	Primaria	Identificador para cada plataforma o modelo de equipos de la red ingresados al inventario	ssradmin_tipoequipos
Descripción de la plataforma	Descripción	nvarchar(100)	No	Descripción para cada plataforma existente	ssradmin_tipoequipos

Tabla 4.1.3.2 Diccionario de datos para la administración de equipos de red

Nombre	Acrónimo	Tipo y Longitud	Llave	Descripción	Tabla
Dirección IP	IP	nvarchar(16)	Primaria	Dirección IP del equipo de red registrado en el inventario	ssradmin_integraciones
Nombre de red	Nombre	nvarchar(255)	No	Nombre que tiene asociado el equipo en la red.	ssradmin_integraciones
Fecha de integración	Fecha_Integ	Fecha	No	Fecha en la que el equipo se dio de alta en el invetnario	ssradmin_integraciones
Modelo o plataforma	Modelo	nvarchar(15)	Foránea	Identificador de la plataforma del equipo registrado	ssradmin_integraciones
Contraseña de Acceso 1	Password1	nvarchar(15)	No	Contraseña 1 de acceso local del equipo si este no cuenta con autenticación por servidor externo.	ssradmin_integraciones
Contraseña de Acceso 2	Password2	nvarchar(15)	No	Contraseña 2 de acceso local del equipo si este no cuenta con autenticación por servidor externo.	ssradmin_integraciones
Estatus de operación de equipo	Status	nvarchar(10)	No	Estatus actual de operación del equipo. Por ejemplo: Activo	ssradmin_integraciones

Tabla 4.1.3.2 Diccionario de datos para la administración de equipos de red (Continuación)

Administración de incidentes de seguridad

En la tabla 4.1.3.3 se presenta el diccionario de datos utilizado en la administración y seguimiento de incidentes de seguridad.

Nombre	Acrónimo	Tipo y Longitud	Llave	Descripción	Tabla
Consecutivo	Numero	Entero	No	Consecutivo para tipo de incidentes	ssradmin_tipoataques
Identificador de tipo de incidente	ID	varchar(35)	Primaria	Identificador para los tipos de incidentes que son reportados	ssradmin_tipoataques
Descripción	Descripcion	varchar(255)	No	Descripción del tipo de incidente	ssradmin_tipoataques
Detalle	Detalle	varchar(255)	No	Breve explicación del tipo de incidente	ssradmin_tipoataques
Identificador consecutivo de incidente	ID_Ataque	Entero	Primaria	Número consecutivo de reporte de incidente	ssradmin_ataques
Dirección IP origen	IPAtacante	varchar(16)	Foránea	Dirección IP desde la que proviene el incidente	ssradmin_ataques
Dirección IP de ruteador de acceso	IPAccessRouter	varchar(16)	No	Dirección IP del último ruteador perteneciente a la infraestructura de la empresa	ssradmin_ataques
Dirección IP del ruteador externo	IPExtRouter	varchar(16)	No	Dirección IP del primer ruteador externo que conecta la dirección IP origen	ssradmin_ataques
Nombre del ruteador de acceso	AccessRouter	varchar(255)	No	Nombre del último ruteador perteneciente a la infraestructura de la empresa	ssradmin_ataques
Organización	Cliente	varchar(100)	No	Nombre de la organización que tiene asignada la IP origen del incidente	ssradmin_ataques

Tabla 4.1.3.3 Diccionario de datos para la administración de incidentes

Nombre	Acrónimo	Tipo y Longitud	Llave	Descripción	Tabla
Identificador del tipo de incidente	Tipo_ataque	varchar(35)	Foránea	Identificador del tipo de incidente presentado en el reporte	ssradmin_ataques
Fecha del incidente	Fecha_Ataque	Fecha	No	Fecha en que ocurrió el incidente	ssradmin_ataques
Contacto Técnico	Responsable	varchar(50)	No	Nombre del contacto técnico de la organización .	ssradmin_ataques
Teléfono del contacto	Telefono	varchar(50)	No	Teléfono para contactar al responsable de la IP origen	ssradmin_ataques
Correo electrónico del contacto	Email	varchar(255)	No	Dirección de e-mail para contactar al responsable de la IP origen	ssradmin_ataques
Bandera de notificación	Sent	Entero	No	Indica si el incidente ya fue notificado por correo electrónico	ssradmin_ataques
Bandera de Solución	Solved	Entero	No	Indica si el estado del incidente, es decir, si ya fue resuelto y cerrado.	ssradmin_ataques
Notas	Notas	varchar(255)	No	Observaciones	ssradmin_ataques
Dirección IP origen	IP	Varchar(16)	Primaria	Dirección IP desde la que proviene el incidente	ssradmin_atcomentarios
Notas de seguimiento	Comentario	varchar(4000)	No	Almacena todas las notas de seguimiento de los operadores cuando se atiende un incidente de seguridad	Ssradmin_atcomentarios

Tabla 4.1.3.3 Diccionario de datos para la administración de incidentes (continuación)

4.1.4 Diagrama Entidad-Relación

En el sistema de inventario desarrollado, se utiliza una base de datos con una estructura definida, la cual consta de objetos básicos o entidades, como son los usuarios, los equipos o los incidentes, y que pueden ser distinguidas unas de otras ya que cada una cuenta con diferentes propiedades.

Todas las entidades de la base de datos cuentan con atributos que describen las propiedades de cada una, como son, en el caso de los usuarios, nombre completo o dirección de correo electrónico.

Dentro de la estructura de la base de datos existen relaciones. Una relación es la asociación que existe entre entidades y que describe las acciones que tiene una sobre la otra. Un ejemplo de relaciones en la base de datos es:

- Un usuario pertenece a un grupo, y un grupo cuenta con uno o más usuarios dentro de él.

- Un equipo de red opera bajo una plataforma, y una plataforma se constituye por muchos equipos.

- Un incidente de seguridad tiene un tipo determinado, y de un tipo de incidente se registran muchos casos.

Para establecer una relación entre dos entidades se cuenta con una llave primaria en una de ellas, que es un campo dentro de la tabla correspondiente que servirá como acceso a todo el registro, por lo que no deberá ser nulo y que, existe en la otra entidad como llave foránea, estableciendo de esta forma, la asociación a través de ellas.

La figura 4.1.4.1 muestra el diagrama Entidad-Relación del sistema de inventario de usuarios, equipos e incidentes de seguridad.

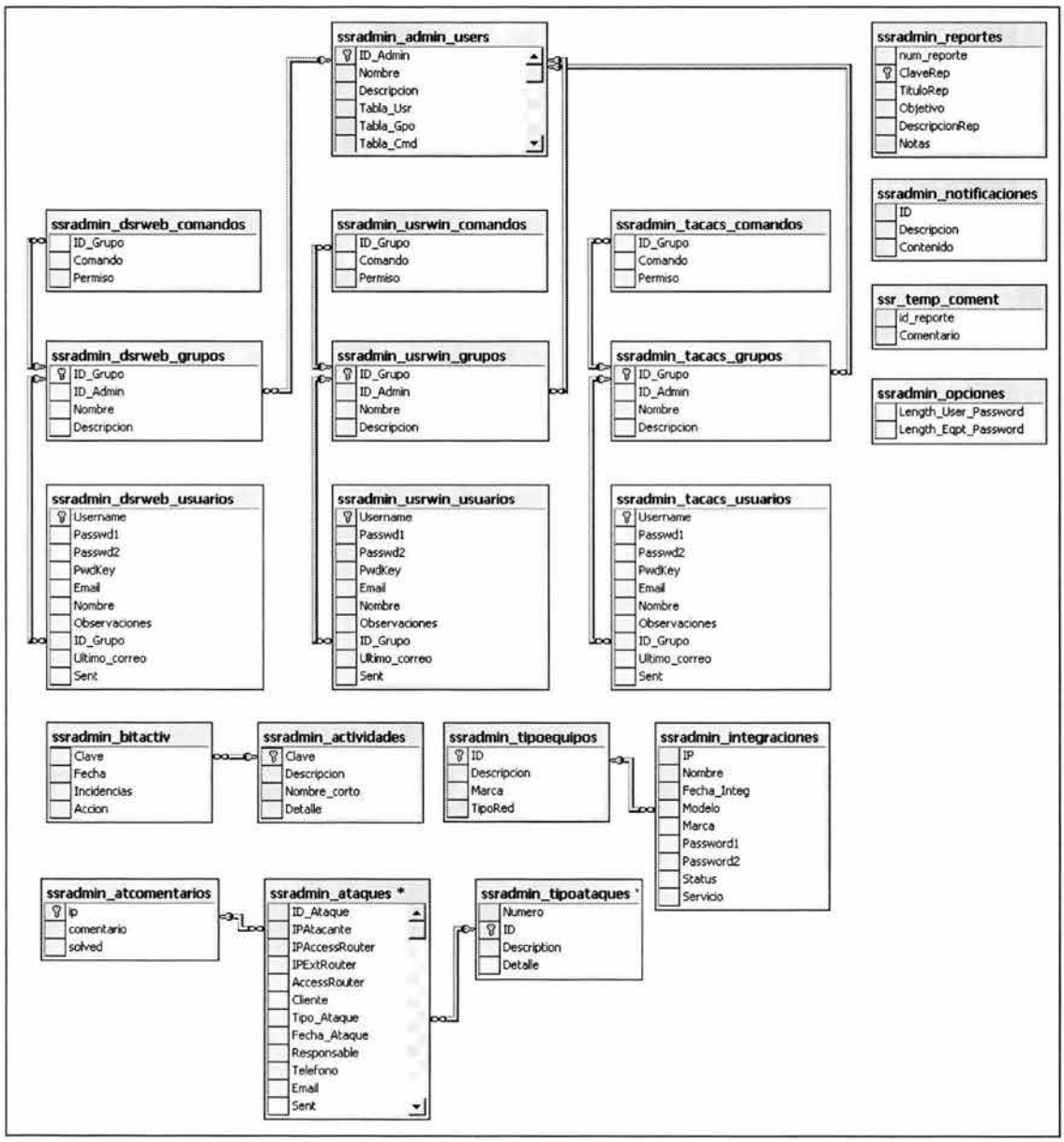


Figura 4.1.4.1 Diagrama Entidad-Relación

4.1.5 Normalización

La normalización es el proceso mediante el cual se transforman datos complejos a una estructura de datos más pequeñas, que además de ser más simples y estables, son más fáciles de mantener. La normalización es una serie de reglas que permiten desarrollar un esquema que minimice los problemas de lógica.

La aplicación de la normalización a la base de datos del sistema de inventario, nos permite eliminar la duplicidad de la información, así como el espacio en disco que nos consume el almacenamiento de la misma. Para ello es necesario la normalización dentro de los tres primeros niveles. La primera, segunda y tercera forma normal (FN1, FN2 y FN3, respectivamente).

Para efectuar este proceso, es necesario una muestra de algunos datos que serán almacenados en SQL Server. Los datos son tomados de la información de los usuarios registrados.

En la tabla 4.1.5.1, se presentan datos de usuarios, grupos y comandos que pueden ejecutar. En un nivel de normalización 0, los datos serían almacenados como se muestra. Se puede visualizar que los usuarios pueden ejecutar un comando 1 y un comando 2 en la plataforma de ruteadores de internet.

El problema se presenta cuando algún usuario necesita ejecutar un comando 3. Si se presentara este caso, se tendría que agregar una columna más, y además reprogramar toda la entrada de datos para que ahora permitiera el campo extra. Cada vez que se necesitara agregar una columna más se tendría que realizar el mismo proceso, lo cual no sería eficiente.

Username	Nombre	Grupo	Descripcion de Grupo	Comando1	Comando2
antogome	Antonio Gomez	CISCO	Usuarios de Cisco	show	clear
esegovia	Eduardo Segoviano	CTEC	Consejo Tecnológico.	erase	write
rsanch	Sanchez Rodriguez	EXTERN	Externos	traceroute	debug
agiron	José Giron	CONF	Configuraciones	reload	show configuration
ecarrada	Edgar Carrada	CLI	Fallas Clientes	login	loopback
mherrea	Mireya Herrera	CONF	Configuraciones	reload	show configuration
vmanriq	Victor Manrique	EXTERN	Externos	traceroute	debug
rantonio	Roberto Jimenez	CLI	Fallas Clientes	login	loopback
jecastil	Jorge Vergara	PROB	Problemas Internet	debug ip packet	enable password
auditcisco	Auditoria de Cisco	MON	Monitoreo	terminal monitor	debug all
rruiz	Rodolfo Ruiz	SOPTE	Soporte	show running-config	show interface
jbarraga	Armando Barragan	INFRA	Infraestructura de red	copy tftp	shutdown
eroguez	Esteban Rodriguez	ING	Ingeniería	configure terminal	no interface
gesparza	Guillermo Esparza	SIS	Sistemas de Gestión	write erase	show ip
maortega	Manuel Ortega	SEG	Seguridad Informática	access-list	ip access-group
aeyebra	Arturo Estrada	SEG	Seguridad Informática	access-list	ip access-group
make	Manuel Ake	SIS	Sistemas de Gestión	write erase	show ip
alanuza	Antonio Lanuza	INFRA	Infraestructura de red	configure terminal	no interface
mmartinr	Miguel Martinez	INFRA	Infraestructura de red	configure terminal	no interface
monsel	Montserrat Luna	CAT	Centro de Atención Telefónica	show startup-config	show version

Tabla 4.1.5.1 Datos con nivel de normalización 0

Primera Forma Normal (FN1)

Para que los datos cumplan con la primera forma normal es necesario:

- Eliminar los datos repetitivos de las tablas individuales
- Crear una tabla separada para cada grupo de datos relacionados
- Identificar cada grupo de usuarios relacionados con la llave primaria

Una vez que se aplica la primera forma normal, se tendría una tabla como la mostrada en la figura 4.5.1.5, donde se utiliza el identificador 'username', para diferenciar a cada usuario.

username	Nombre	Grupo	Descripcion de Grupo	Comando
antogome	Antonio Gomez	CISCO	Usuarios de Cisco	show
antogome	Antonio Gomez	CISCO	Usuarios de Cisco	clear
esegovia	Eduardo Segoviano	CTEC	Consejo Tecnológico.	erase
esegovia	Eduardo Segoviano	CTEC	Consejo Tecnológico.	write
rsanch	Sanchez Rodriguez	EXTERN	Externos	traceroute
rsanch	Sanchez Rodriguez	EXTERN	Externos	debug
agiron	José Giron	CONF	Configuraciones	reload
agiron	José Giron	CONF	Configuraciones	show configuration
ecarrada	Edgar Carrada	CLI	Fallas Clientes	login
ecarrada	Edgar Carrada	CLI	Fallas Clientes	loopback
mherrea	Mireya Herrera	CONF	Configuraciones	reload
mherrea	Mireya Herrera	CONF	Configuraciones	show configuration
vmanriq	Victor Manrique	EXTERN	Externos	traceroute
vmanriq	Victor Manrique	EXTERN	Externos	debug
rantonio	Roberto Jimenez	CLI	Fallas Clientes	login
rantonio	Roberto Jimenez	CLI	Fallas Clientes	loopback
jecastil	Jorge Vergara	PROB	Problemas Internet	debug ip packet
jecastil	Jorge Vergara	PROB	Problemas Internet	enable password
auditcisco	Auditoria de Cisco	MON	Monitoreo	terminal monitor
auditcisco	Auditoria de Cisco	MON	Monitoreo	debug all
rruiz	Rodolfo Ruiz	SOPTE	Soporte	show running-config
rruiz	Rodolfo Ruiz	SOPTE	Soporte	show interface
jbarraga	Armando Barragan	INFRA	Infraestructura de red	copy tftp
jbarraga	Armando Barragan	INFRA	Infraestructura de red	shutdown
eroguez	Esteban Rodriguez	ING	Ingeniería	configure terminal
eroguez	Esteban Rodriguez	ING	Ingeniería	no interface
gesparza	Guillermo Esparza	SIS	Sistemas de Gestión	write erase
gesparza	Guillermo Esparza	SIS	Sistemas de Gestión	show ip
maortega	Manuel Ortega	SEG	Seguridad Informática	access-list
maortega	Manuel Ortega	SEG	Seguridad Informática	ip access-group
aeyebra	Arturo Estrada	SEG	Seguridad Informática	access-list
aeyebra	Arturo Estrada	SEG	Seguridad Informática	ip access-group
make	Manuel Ake	SIS	Sistemas de Gestión	write erase
make	Manuel Ake	SIS	Sistemas de Gestión	show ip
alanuza	Antonio Lanuza	INFRA	Infraestructura de red	configure terminal
alanuza	Antonio Lanuza	INFRA	Infraestructura de red	no interface
mmartinr	Miguel Martinez	INFRA	Infraestructura de red	configure terminal
mmartinr	Miguel Martinez	INFRA	Infraestructura de red	no interface
monsel	Montserrat Luna	CAT	Centro de Atención Telefónica	show startup-config
monsel	Montserrat Luna	CAT	Centro de Atención Telefónica	show version

Tabla 4.1.5.2 Datos después de aplicar FN1

Una vez que se aplicó la primera forma normal se soluciona el problema referente a la limitación del campo Comando, sin embargo se puede notar que cada vez que se

agrega un nuevo registro a la tabla, se duplica el campo de descripción de grupo y username, lo que podría provocar problemas de espacio, por toda la rapidez con la que la tabla crecería. Dada esta situación se aplica la segunda forma normal.

Segunda Forma Normal (FN2)

Para la segunda forma normal es necesario:

- Crear tablas separadas para los campos que se aplican a varios registros.
- Relacionar las tablas mediante una clave externa.

De esta forma separamos el campo de Descripción de grupo, de tal forma que puedan agregarse más en el futuro sin necesidad de duplicar los demás datos. Se utiliza el campo Grupo como llave primaria para relacionar los campos. Las tablas resultantes son la 4.1.5.3 y 4.1.5.4.

Grupo	Descripcion de Grupo
CISCO	Usuarios de Cisco
CTEC	Consejo Tecnológico.
EXTERN	Externos
CONF	Configuraciones
CLI	Fallas Clientes
CONF	Configuraciones
EXTERN	Externos
CLI	Fallas Clientes
PROB	Problemas Internet
MON	Monitoreo
SOPTE	Soporte
INFRA	Infraestructura de red
ING	Ingeniería
SIS	Sistemas de Gestión
SEG	Seguridad Informática
SIS	Sistemas de Gestión
INFRA	Infraestructura de red
CAT	Centro de Atención Telefónica

Tabla 4.1.5.3 Tabla de grupos

username	Nombre	Grupo	Comando
antogome	Antonio Gomez	CISCO	show
antogome	Antonio Gomez	CISCO	clear
esegovia	Eduardo Segoviano	CTEC	erase
esegovia	Eduardo Segoviano	CTEC	write
rsanch	Sanchez Rodriguez	EXTERN	traceroute
rsanch	Sanchez Rodriguez	EXTERN	debug
agiron	José Giron	CONF	reload
agiron	José Giron	CONF	show configuration
ecarrada	Edgar Carrada	CLI	login
ecarrada	Edgar Carrada	CLI	loopback
mherrea	Mireya Herrera	CONF	reload
mherrea	Mireya Herrera	CONF	show configuration
vmanriq	Victor Manrique	EXTERN	traceroute
vmanriq	Victor Manrique	EXTERN	debug
rantonio	Roberto Jimenez	CLI	login
rantonio	Roberto Jimenez	CLI	loopback
jecastil	Jorge Vergara	PROB	debug ip packet
jecastil	Jorge Vergara	PROB	enable password
auditcisco	Auditoria de Cisco	MON	terminal monitor
auditcisco	Auditoria de Cisco	MON	debug all
rruiz	Rodolfo Ruiz	SOPTE	show running-config
rruiz	Rodolfo Ruiz	SOPTE	show interface
jbarraga	Armando Barragan	INFRA	copy tftp
jbarraga	Armando Barragan	INFRA	shutdown
eroguez	Esteban Rodriguez	ING	configure terminal
eroguez	Esteban Rodriguez	ING	no interface
gesparza	Guillermo Esparza	SIS	write erase
gesparza	Guillermo Esparza	SIS	show ip
maortega	Manuel Ortega	SEG	access-list
maortega	Manuel Ortega	SEG	ip access-group
aeyebra	Arturo Estrada	SEG	access-list
aeyebra	Arturo Estrada	SEG	ip access-group
make	Manuel Ake	SIS	write erase
make	Manuel Ake	SIS	show ip
alanuza	Antonio Lanuza	INFRA	configure terminal
alanuza	Antonio Lanuza	INFRA	no interface
mmartinr	Miguel Martinez	INFRA	configure terminal
mmartinr	Miguel Martinez	INFRA	no interface
monsel	Montserrat Luna	CAT	show startup-config
monsel	Montserrat Luna	CAT	show version

Tabla 4.1.5.4 Tabla de usuarios.

De esta forma logramos crear una tabla de grupo, en donde las descripciones ya no se repiten. Sin embargo si deseamos agregar un comando a un usuario, se duplicarán

nuevamente los campos de username y grupo simultáneamente, por lo que es necesario aplicar la tercera forma normal para separar los comandos a una tabla independiente.

Tercera Forma Normal (FN3)

Para la tercera forma normal es necesario:

- Eliminar los campos que no dependan de la llave.

Entonces en la tabla de usuario, se puede separar el campo comando y almacenarlo en la tercer tabla. De esta forma, la información quedaría almacenada como se muestra en las tablas 4.1.5.5, 4.1.5.6 y 4.1.5.7.

username	**Nombre**	**Grupo**
antogome	Antonio Gomez	CISCO
esegovia	Eduardo Segoviano	CTEC
rsanch	Sanchez Rodriguez	EXTERN
agiron	José Giron	CONF
ecarrada	Edgar Carrada	CLI
mherrea	Mireya Herrera	CONF
vmanriq	Victor Manrique	EXTERN
rantonio	Roberto Jimenez	CLI
jecastil	Jorge Vergara	PROB
auditcisco	Auditoria de Cisco	MON
rruiz	Rodolfo Ruiz	SOPTE
jbarraga	Armando Barragan	INFRA
eroguez	Esteban Rodriguez	ING
gesparza	Guillermo Esparza	SIS
maortega	Manuel Ortega	SEG
aeyebra	Arturo Estrada	SEG
make	Manuel Ake	SIS
alanuza	Antonio Lanuza	INFRA
mmartinr	Miguel Martinez	INFRA
monsel	Montserrat Luna	CAT

Tabla 4.1.5.5 Tabla de usuarios

Grupo	**Descripcion de Grupo**
CISCO	Usuarios de Cisco
CTEC	Consejo Tecnológico.
EXTERN	Externos
CONF	Configuraciones
CLI	Fallas Clientes
CONF	Configuraciones
EXTERN	Externos
CLI	Fallas Clientes
PROB	Problemas Internet
MON	Monitoreo
SOPTE	Soporte
INFRA	Infraestructura de red
ING	Ingeniería
SIS	Sistemas de Gestión
SEG	Seguridad Informática
SIS	Sistemas de Gestión
INFRA	Infraestructura de red
CAT	Centro de Atención Telefónica

Tabla 4.1.5.6 Tabla de Grupos

Grupo	Comando
SEG	access-list
CISCO	clear
ING	configure terminal
INFRA	configure terminal
INFRA	copy tftp
EXTERN	debug
MON	debug all
PROB	debug ip packet
PROB	enable password
CTEC	erase
SEG	ip access-group
CLI	login
CLI	loopback
ING	no interface
INFRA	no interface
CONF	reload
CISCO	show
CONF	show configuration
SOPTE	show interface
SIS	show ip
SOPTE	show running-config
CAT	show startup-config
CAT	show version
INFRA	shutdown
MON	terminal monitor
EXTERN	traceroute
CTEC	write
SIS	write erase

Figura 4.1.5.7 Tabla de comandos

De esta forma, se tiene la llave primaria Grupo en la tabla de grupos relacionada con la llave foránea Grupo en la tabla de usuarios, de tal forma que no importa cuántos registros se agreguen, la descripción del grupo sólo es almacena una vez. En la tabla de comandos, ahora la llave primaria está formada en conjunto por el campo ID_Grupo y Comando de tal forma que no es posible duplicar ambos campos simultáneamente.

Una vez realizada la normalización, se completa la creación de las tablas con los campos adicionales que requerirá cada una de ellas, de acuerdo a la información que será almacenada.

4.2 DISEÑO Y CONSTRUCCIÓN DEL BACK-END

El Back-End del sistema está constituido principalmente por la base de datos, la cual está instalada en un servidor Microsoft Windows 2000 Server, y sobre el DBMS de Microsoft SQL Server 2000 en su edición Standard. Para la instalación de SQL Server se verificó que el servidor contara con los requerimientos de hardware necesarios, para que el rendimiento fuera el más óptimo posible.

Posteriormente, se procedió a realizar la instalación de Microsoft SQL Server 2000 Standard Edition, estableciendo ciertos parámetros especiales durante la instalación, necesarios para la operación de la base de datos.

En la figura 4.2.1, se muestra la pantalla inicial para la instalación del manejador de la base de datos, y en la cual se selecciona la opción de instalación de los Componentes de SQL Server 2000 (SQL Server 2000 Components).

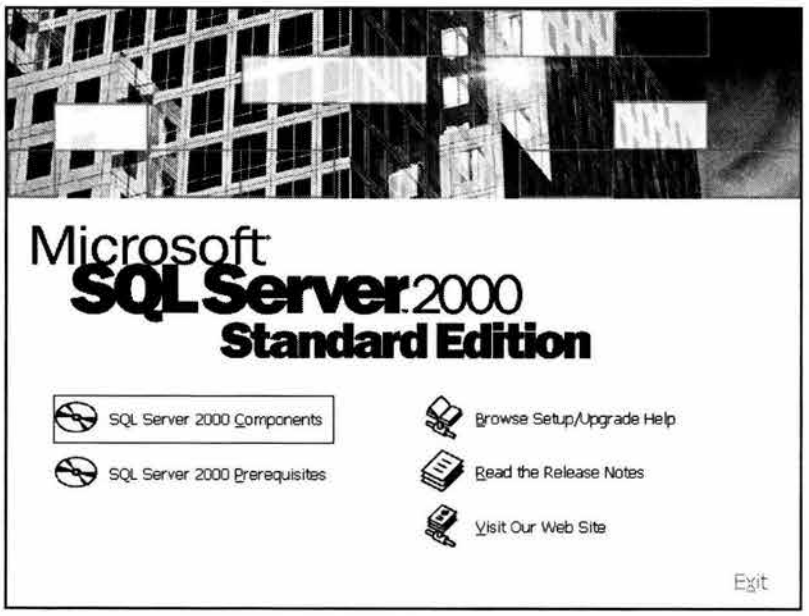


Figura 4.2.1. Pantalla inicial para la instalación de SQL Server 2000

Posteriormente, es seleccionada la opción que nos permite instalar el servidor de base de datos (Install Database Server) en el sistema, como se muestra en la figura 4.2.2.

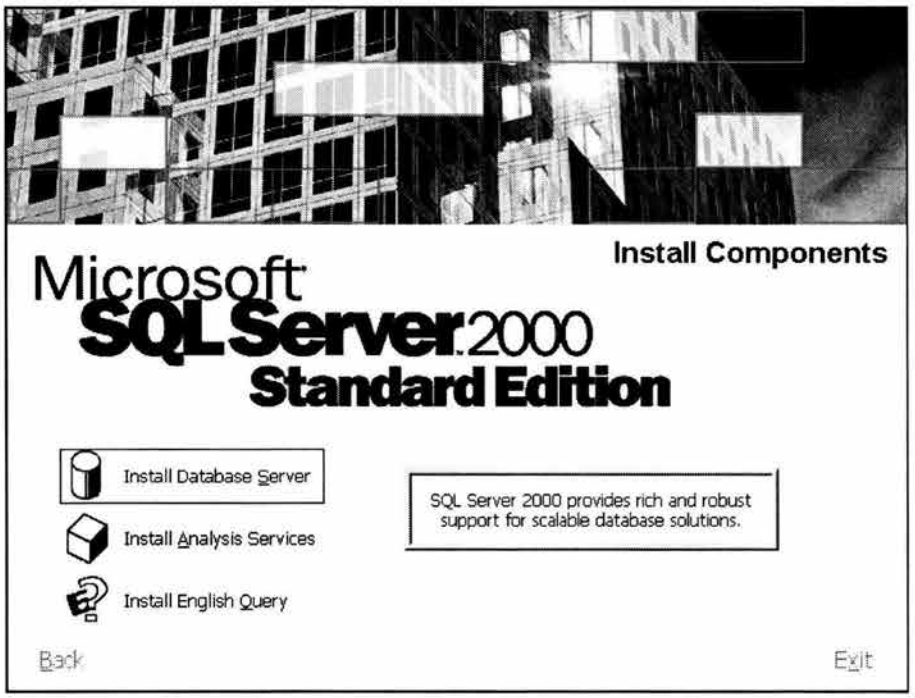


Figura 4.2.2 Selección de instalación del servidor de base de datos.

Una vez que se inicia la instalación, se deben tener presentes las características que tendrá la base de datos y bajo las cuales va a operar, esto debido a que SQL Server nos proporciona varias opciones diferentes de instalación, y la elegida es la que quedará configurada.

La base de datos se instalará y operará en el servidor local, ya que la administración de él se realiza en la consola del mismo y no remotamente, por lo que se le indicará a la instalación como se especifica en la figura 4.2.3, en la que también se muestra el nombre de red del servidor en el cual se está ejecutando la instalación. Este nombre lo detecta automáticamente el programa de instalación de acuerdo al que está configurado en Windows 2000 Server y solo se puede modificar si se va a instalar en un servidor remoto.

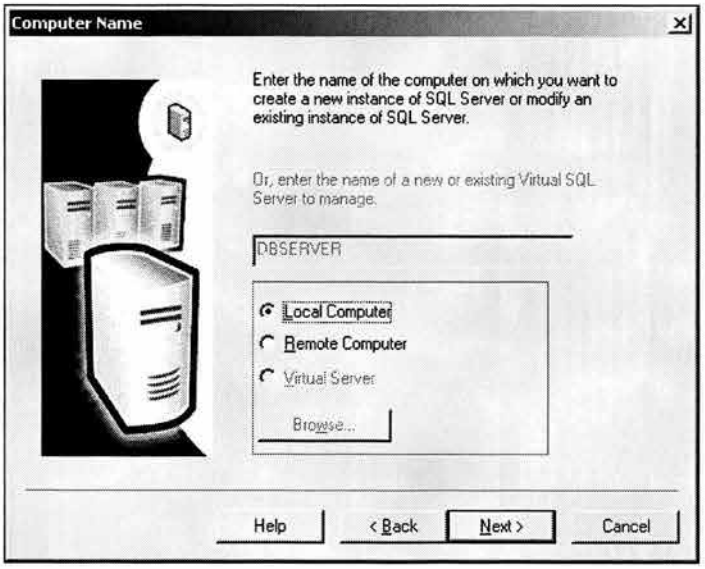


Figura 4.2.3 Instalación en servidor local.

En la figuras 4.2.4 y 4.2.5, se muestra la parte del asistente en el que se indica que se instale la opción predeterminada, y la cual consta del motor de la base de datos y las herramientas de cliente, necesarias para la administración.

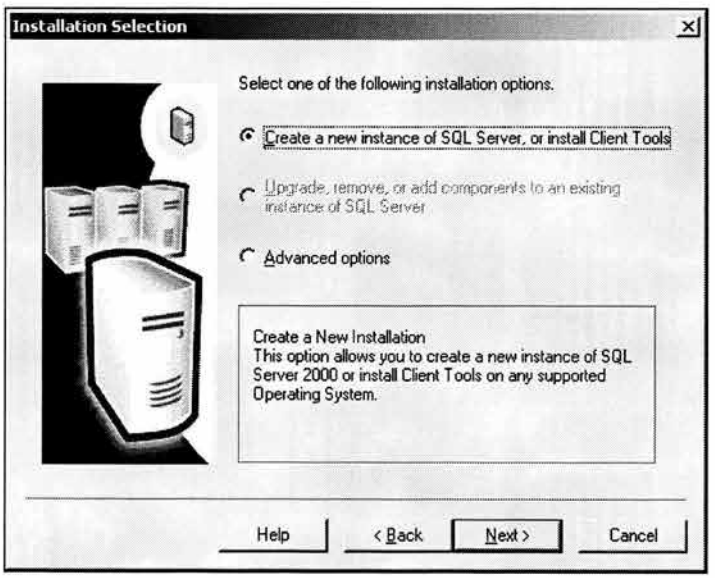


Figura 4.2.4 Instalación de SQL Server y las herramientas de cliente.

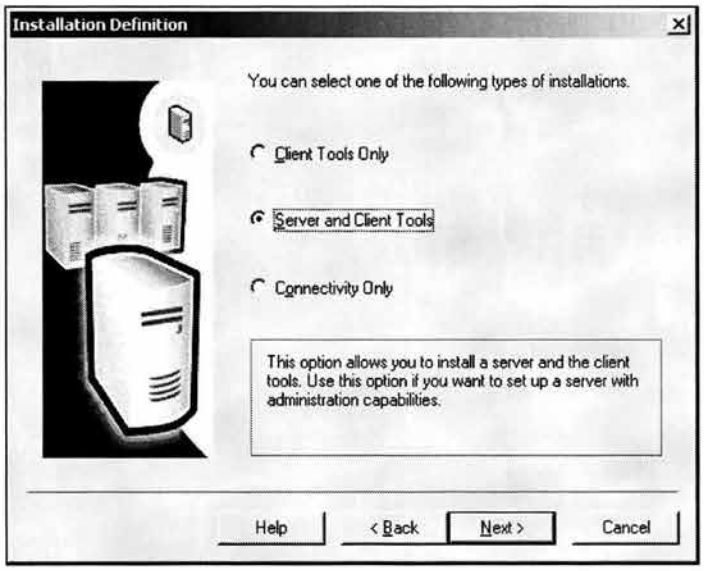


Figura 4.2.5 Instalar servidor y herramientas de cliente

Posteriormente, se escribe el nombre de la empresa y del propietario del servidor como se hace en la mayoría de las instalaciones que se ejecutan en los sistemas Windows, así como la aceptación del contrato de licencia de uso del software.

Es recomendable seleccionar una instalación personalizada de los componentes elegidos en las pantallas anteriores, para revisar cada uno de los elementos que serán instalados en el sistema, y en caso de existir alguna duda de alguno en especial, consultar la documentación y en base a ellos elegir si se instala o no. En la mayoría de los casos, se pueden dejar los elementos que se muestran al seleccionar está opción como los que están marcados por defecto, pero aún así, en estos casos es útil para revisar y saber lo que será cargado en el sistema. Los directorios de instalación se dejan preferentemente a los que el instalador indica.

En las figuras 4.2.6 y 4.2.7 podemos ver la personalización de estas opciones.

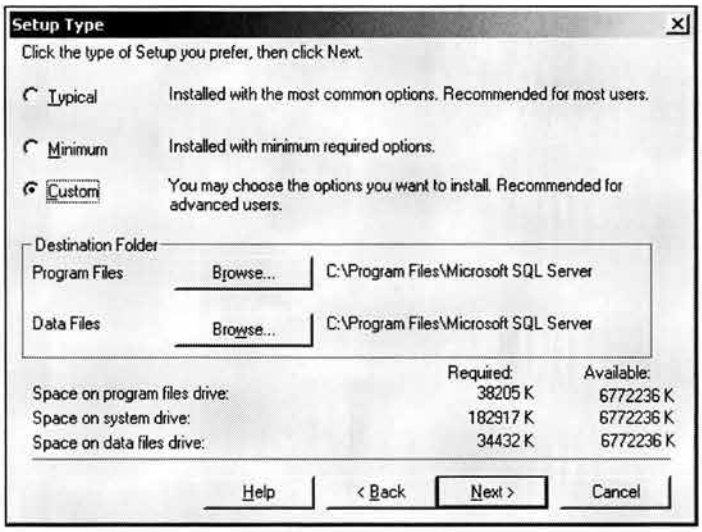


Figura 4.2.6 Selección de instalación personalizada.

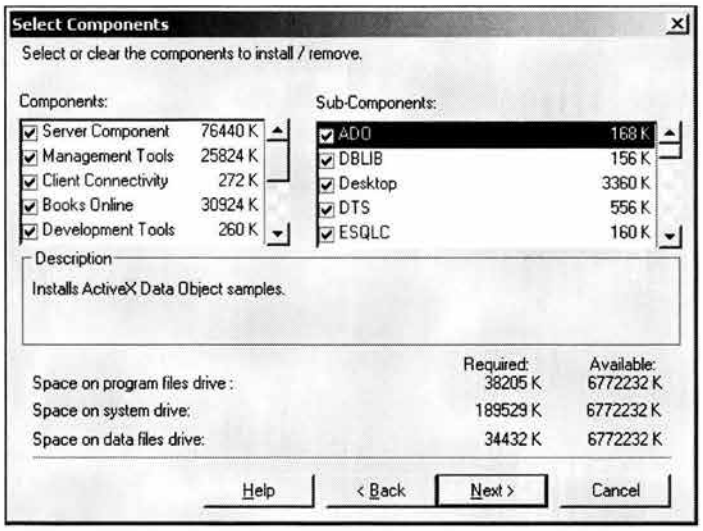


Figura 4.2.7. Elementos de la instalación personalizada.

Otro parámetro importante a configurar durante la instalación es el dueño de los procesos que correrán al quedar instalado el servidor, que son los servicios de SQL Server y el agente SQL Server, el cual es útil para monitorear los servicios y operaciones, replicación, bitácoras y tareas, o bien para iniciar otros procesos como respaldos automáticos. Es posible indicarle la cuenta existente en algún dominio, pero

en este caso, como no se cuenta con un dominio y esta base de datos correrá de manera local, como se mencionó anteriormente, se le indica que pueda ser ejecutado bajo alguna cuenta configurada localmente en Windows 2000 Server. En las figuras 4.2.8 y 4.2.9 se muestra la configuración que se realiza en la instalación para este aspecto.

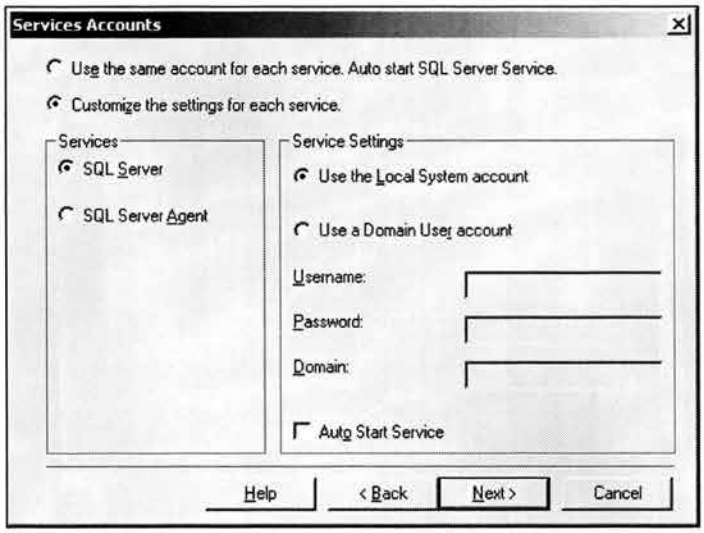


Figura 4.2.8 Configuración del servicio de SQL Server

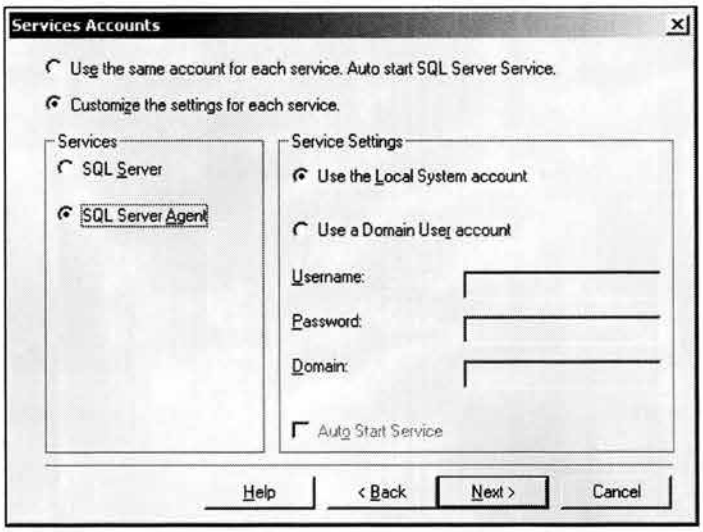


Figura 4.2.9 configuración del proceso para el Agente de SQL Server

Es importante saber que esta cuenta es la que se utiliza para administrar los procesos de SQL como tales, que se ejecutan en Windows 2000, y no como la cuenta de administrador de base de datos.

La cuenta para la administración de la base de datos es asignada a un usuario llamado sa (System Administrator), y puede configurarse de dos maneras:

- Método de Autenticación por Windows, en la cual un usuario se conecta a la base de datos por medio de una cuenta dada de alta en Windows 2000. SQL Server valida el nombre de la cuenta y la contraseña contra lo que tiene configurado el sistema operativo.

- Método de Autenticación Mixta, en la cual se puede hacer uso de la autentificación por Windows o bien por SQL Server. Los usuarios que se conectan a través de Windows pueden hacer uso de conexiones de confianza (conexiones validadas por Windows) tanto en modo mixto como en autentificación por Windows. La autentificación por SQL Server se utiliza para compatibilidad.

En este caso, se elige la opción de autenticación mixta, y en la cual es necesaria la cuenta de administración del sistema (sa). En este paso de la instalación se debe especificar la contraseña para dicha cuenta y, aunque el programa de instalación permite la opción de usarla sin contraseña (contraseña en blanco), no es recomendable, debido a que puede dejar al servidor vulnerable, teniendo acceso cualquier persona desde cualquier lugar, pudiendo obtener el control de la máquina y de la base de datos.

Para este caso, se configura una contraseña de acceso de ocho caracteres de longitud y alfanumérica.

En la figura 4.2.10 se presenta la pantalla de configuración para la cuenta de sa.

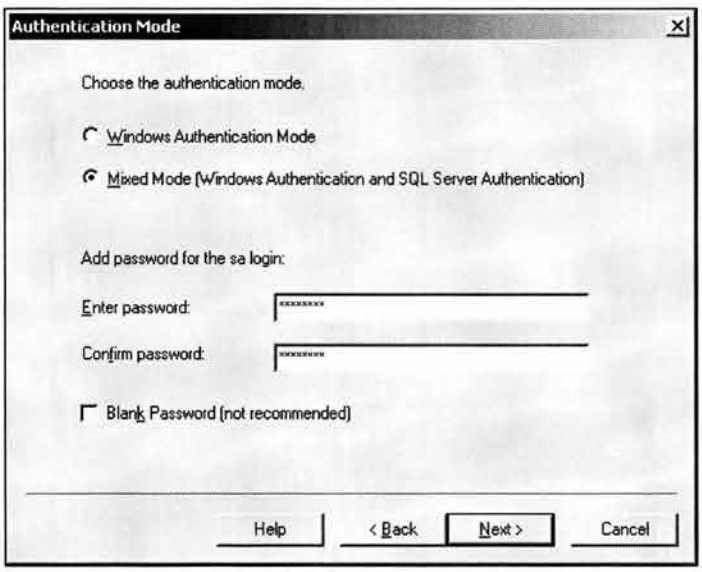


Figura 4.2.10 Configuración de la contraseña para cuenta sa.

La configuración de caracteres se deja preferentemente en la opción predeterminada, es decir, con texto no sensible a mayúsculas y minúsculas para evitar los problemas derivados de ello.

A continuación se configura el método de comunicación en red. Debido a que la aplicación trabaja en un ambiente de red, entonces se configura utilizando el protocolo TCP/IP, y en el cual se especifica el puerto TCP sobre el cual se establecerá la conexión desde las terminales o clientes hacia el servidor de SQL 2000. La instalación predetermina el puerto 1433 de TCP, y es recomendable no cambiarlo, sin embargo también el programa de instalación predetermina la comunicación por Named Pipes el cual es un protocolo de comunicación propietario de Microsoft. En nuestro caso no lo seleccionamos y configuramos la comunicación únicamente por TCP como se ve en la figura 4.2.11, con el puerto mencionado y sin el uso de un servidor proxy, ya que no se cuenta con él.

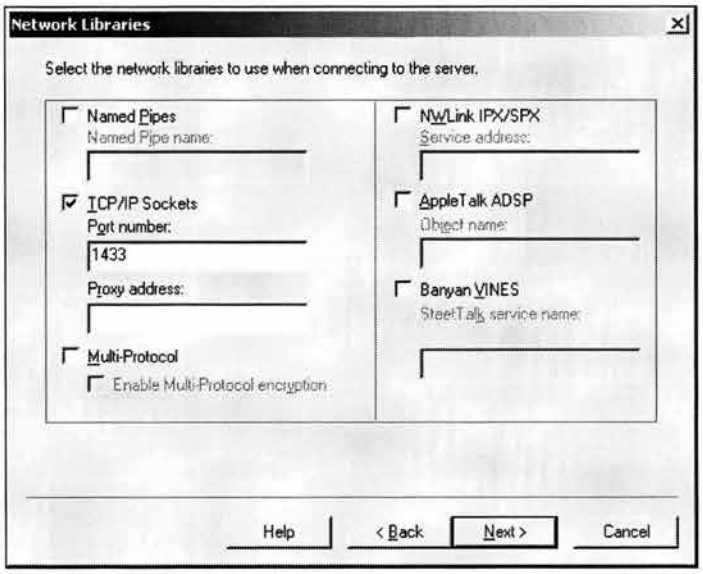


Figura 4.2.11 Configuración del método de comunicación por red.

Posteriormente a la especificación de todos los parámetros de instalación, se procede a la copia de archivos al servidor y a la configuración de los servicios necesarios. En la figura 4.2.12 se presenta el final de la instalación.

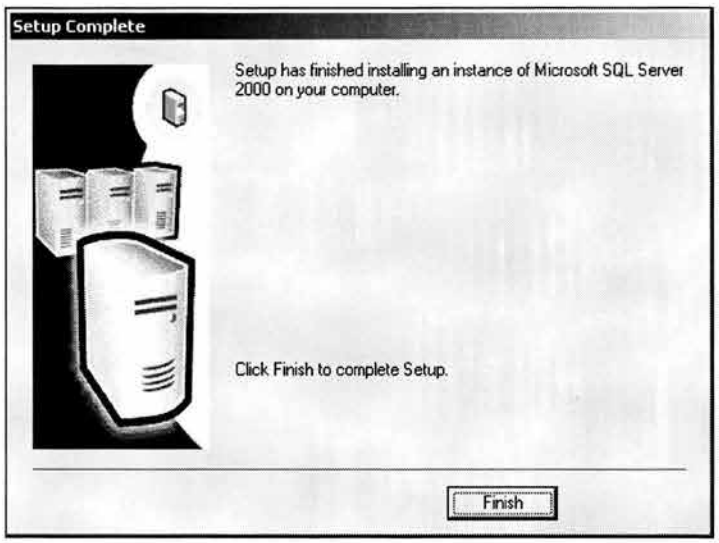


Figura 4.2.12. Finalización de la instalación

Una vez terminada la instalación se reinicia el equipo, teniéndose ya los servicios de SQL Server ejecutándose en el sistema como se ve en la figura 4.2.13.

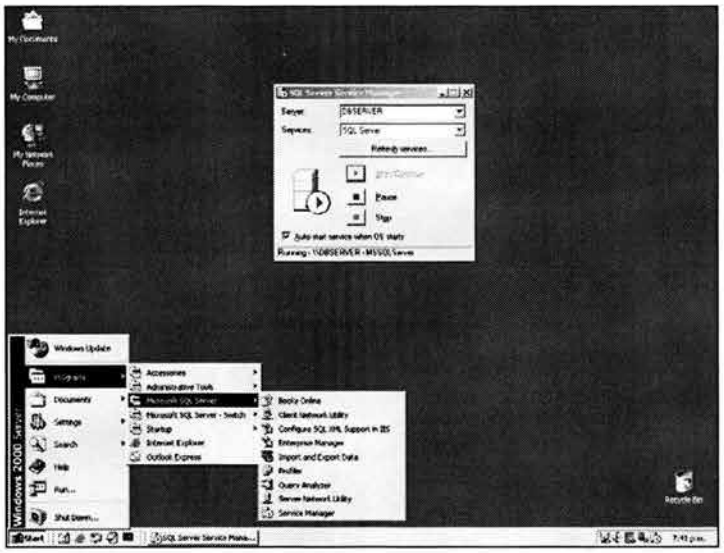


Figura 4.2.13 Servicios de SQL Server 2000 instalados.

Podemos ver la existencia de SQL Server en los elementos del menú de inicio, y los procesos ejecutándose en el administrador de servicios de SQL (SQL Server Service Manager) y en la barra de íconos junto al reloj del sistema.

Una vez realizada la instalación del SQL Server 2000, se procede a crear la base de datos que el sistema de inventarios e incidentes de seguridad hará uso. Para este proceso se hace uso de las herramientas de cliente que se seleccionaron durante la instalación, y específicamente del Administrador de Base de Datos de SQL Server (Microsoft SQL Server Enterprise Manager), y mediante el cual realizan las siguientes actividades relacionadas con la administración de las bases de datos.

- Definición de grupos de servidores donde se ejecuta SQL Server.

- Configuración de las opciones de operación de los servidores de SQL Server que se tienen registrados.

- Creación y administración de todas las bases de datos de SQL Server, objetos, cuentas de usuarios y permisos para los servidores registrados.

- Definición y ejecución de tareas administrativas de SQL Server.

- Diseño y ejecución de sentencias de SQL Server.

En la figura 4.2.14 se presenta el SQL Server Enterprise Manager. Se pueden observar las bases de datos que crea la instalación. En estas bases de datos se guarda información del servidor SQL, así como ejemplos.

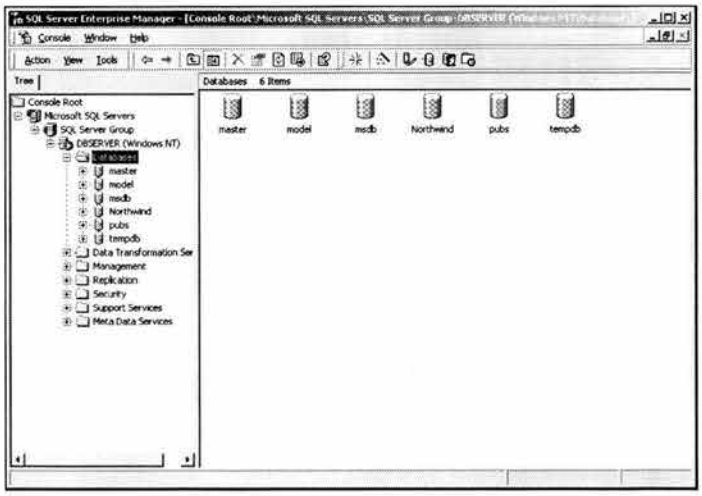


Figura 4.2.14 Microsoft SQL Server 2000 Enterprise Manager.

Se puede observar que el servidor se encuentra registrado en el grupo que la instalación crea de manera predeterminada y debajo de él todas las opciones que pueden ser administradas: bases de datos, servicios de transformación de datos, administración, replicación, seguridad, servicios de soporte y servicios de meta-datos.

La creación de la base de datos para el sistema de inventarios e incidentes de seguridad, se crea utilizando esta herramienta. En la carpeta de bases de datos (Databases) se selecciona la opción 'New Database...', como se ve en la figura 4.2.15.

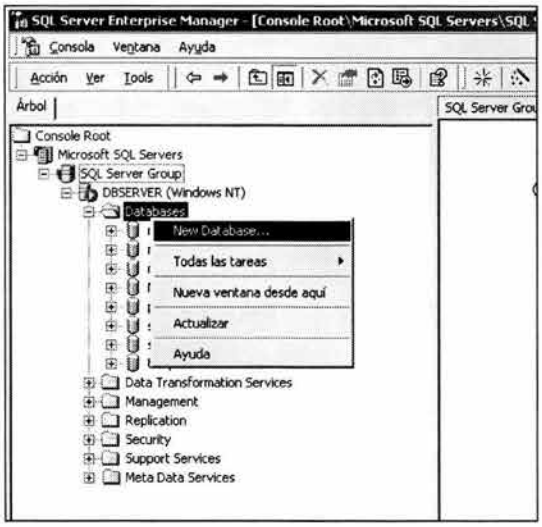


Figura 4.2.15 Creación de la base de datos.

Los parámetros principales que se deben especificar para la creación de una nueva base de datos son:

- Nombre, el cual es el identificador de la base de datos. Con él se hará referencia para realizar las conexiones desde la aplicación. El cuadro de diálogo para la especificación de este parámetro está mostrado en la figura 4.2.16.

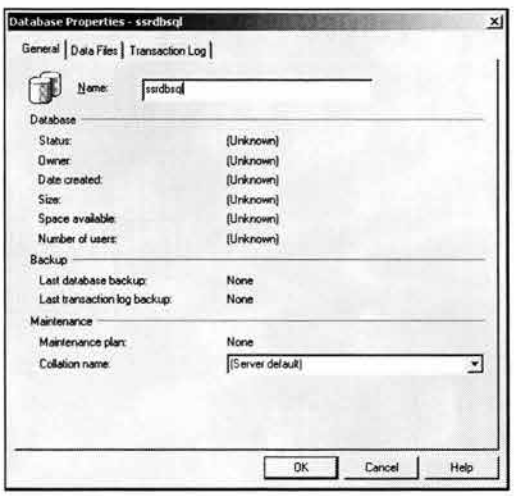


Figura 4.2.16 Especificación del nombre de la base de datos.

El nombre de la base de datos es 'ssrdbsql' y debido a que el sistema pertenecerá al área de seguridad de red del ISP, se obtiene el prefijo 'ssr' o Sistema de Seguridad de Red.

- Archivo de datos, en el cual se almacenará toda la información contenida en tablas, vistas y procedimientos de la base de datos. La ruta de acceso para la creación del archivo por defecto es el directorio de instalación de SQL Server, sin embargo en este caso, se cambia a otra unidad y directorio. El cuadro de diálogo para la especificación de este parámetro está mostrado en la figura 4.2.17. En él podemos ver las opciones de tamaño del archivo, en este caso se especifica un tamaño inicial de 150 MB y no se elige la opción de Automatically Grow File (crecer automáticamente el archivo), para evitar que el crecimiento sea desmedido y se utilice espacio innecesario en disco.

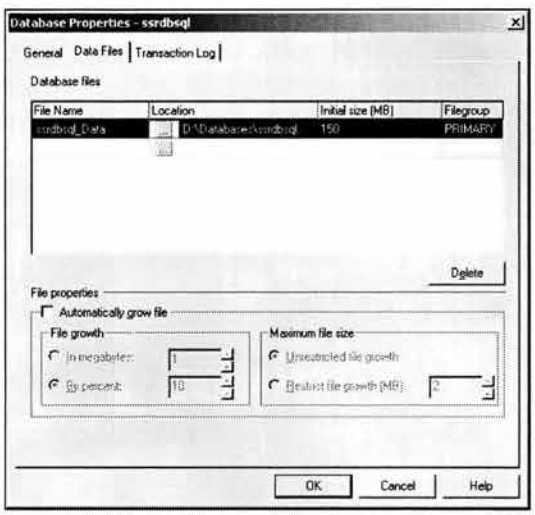


Figura 4.2.17 Configuración inicial del archivo de datos.

- Archivo de transacciones, que almacenan toda las transacciones que se hacen a la base de datos cuando es ejecutada una consulta o sentencia SQL en ella será creado de 50MB . Los parámetros para el archivo como ruta de acceso, y otras

opciones se especifican igual que para el archivo de datos y se ve en la figura 4.2.18.

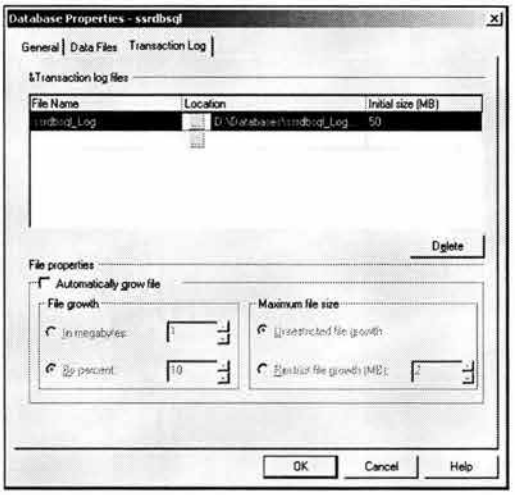


Figura 4.2.18 Configuración inicial del archivo de transacciones.

Para crear la base de datos, se aceptan los parámetros establecidos y se presiona OK en el cuadro de diálogo. Una vez creada la base de datos 'ssrdbsql', podemos verla en el explorador del Enterprise Manager como en la figura 4.2.19.

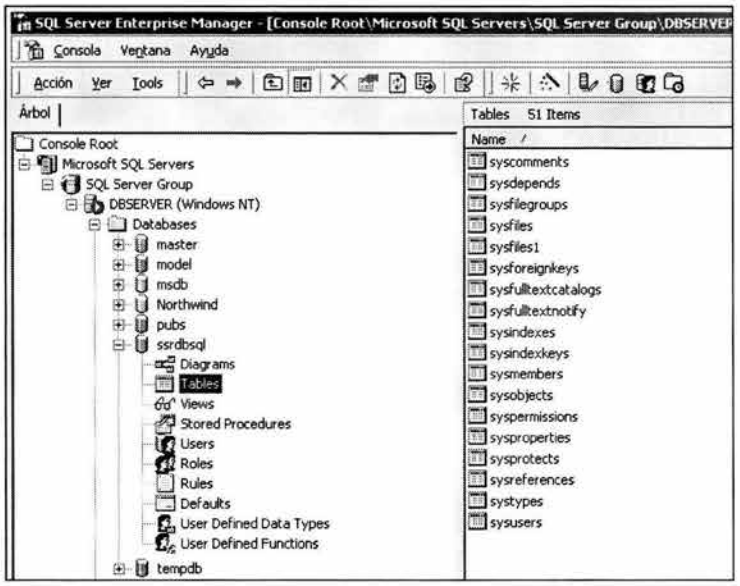


Figura 4.2.19 Visualización de la base de datos ssrdbsql creada.

Ya que la base de datos para el sistema se encuentra creada, entonces se procede a crear cada una de las tablas necesarias para el almacenamiento del inventario de equipos, usuarios e incidentes de seguridad, así como toda la información que de esto se derive.

Para la creación de una tabla, existen dos procedimientos diferentes.

- Gráficamente, en donde se especifica en el Enterprise Manager, mediante el uso de ventanas. Seleccionando el nombre de la base de datos ssrdbsql abre un árbol con todos los elementos que forman parte de ella como son diagramas, tablas, vistas, procedimientos almacenados, usuarios, roles, reglas, restricciones, tipos de datos de usuario y funciones de usuarios. Al abrir el menú contextual del elemento **Tables** (Tablas), se selecciona la opción '**New Table...**' (Nueva Tabla), para abrir el cuadro de dialogo que nos permite especificar las columnas y sus definiciones. En la figura 4.2.20 se observa la creación de la tabla 'ssradmin_integraciones', en la cual se almacenará la información correspondiente a los equipos que se integran al inventario.

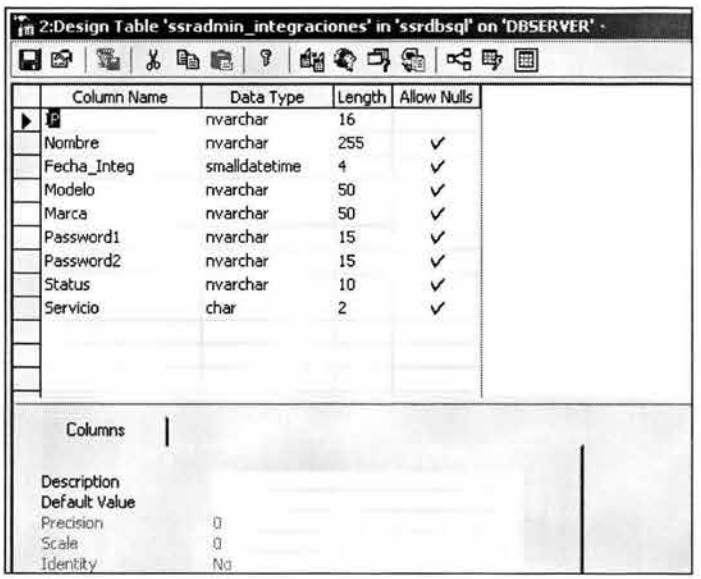


Figura 4.2.20 Creación de la tabla para inventario de equipos.

- Mediante la ejecución un script de T-SQL, en la cual utilizando sentencias de SQL y mediante la herramienta **SQL Query Analyzer** (Analizador de Consultas de SQL), se crea la tabla al ejecutarlo. En la figura 4.2.21 se muestra la interfaz de usuario para esta herramienta, y el script que se corre para crear la misma tabla ssradmin_integraciones.

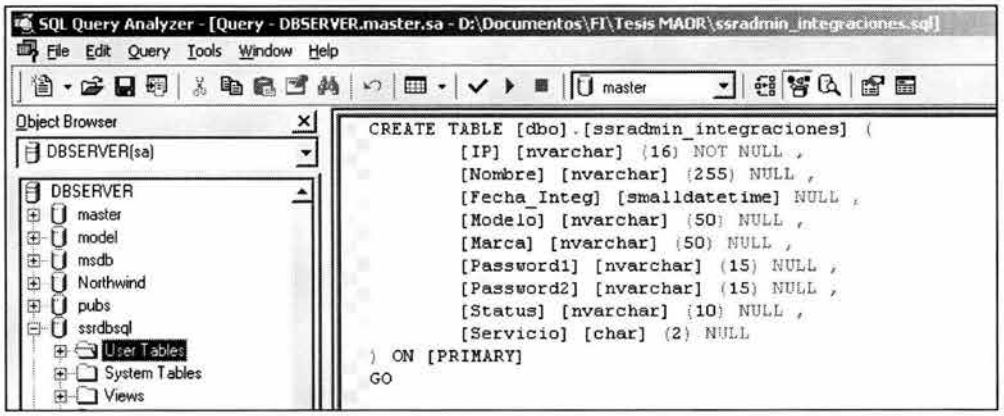


Figura 4.2.21 Creación de la tabla ssradmin_integraciones mediante script.

El proceso gráfico es realizado para la creación de cada una de las tablas que constituyen la base de datos con sus respectivas columnas.

Una herramienta útil es la generación de scripts de SQL, en la cual es posible la construcción de todas las sentencias de T-SQL necesarias para crear toda la estructura de tablas de la base de datos y que es útil para la creación de una réplica del árbol de tablas en otro servidor.

La figura 4.2.22, muestra las tablas ya creadas en la ventana de Enterprise Manager de SQL Server 2000. Estas tablas fueron creadas utilizando el procedimiento descrito anteriormente.

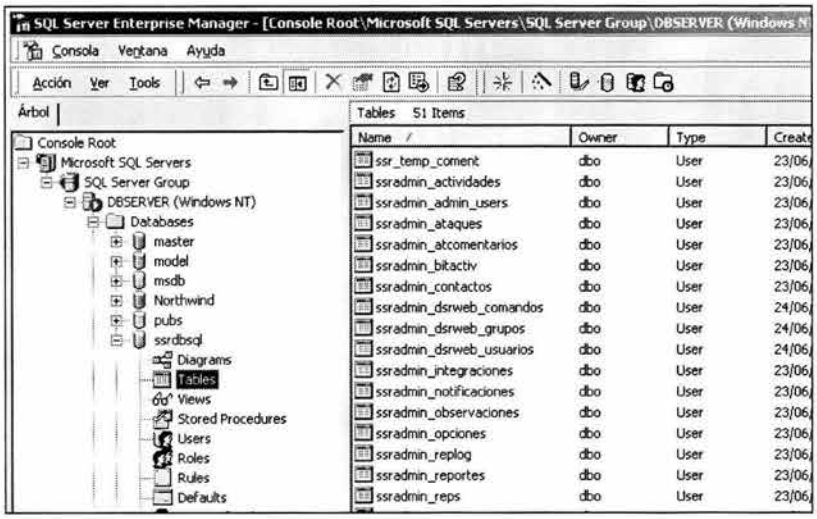


Figura 4.2.22 Tablas de la base de datos del sistema.

Se puede hacer una consulta utilizando el SQL Query Analyzer, seleccionando algunos o todos los registros de las tablas con un comando de T-SQL como se muestra en la figura 4.2.23. Con el Enterprise Manager, se puede hacer una consulta de los registros de en una tabla con la opción Open Table del menú que se muestra al seleccionar una tabla con el botón secundario del ratón. El resultado es como el de la figura 4.2.24.

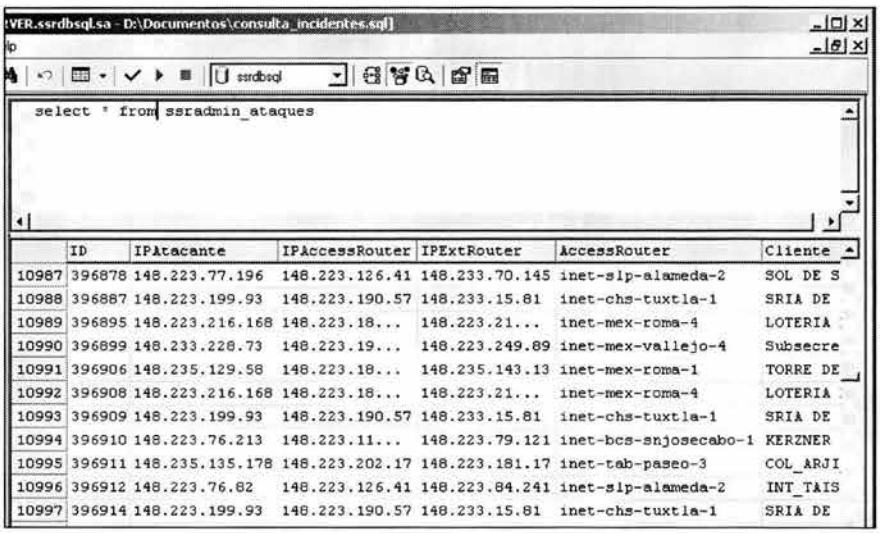
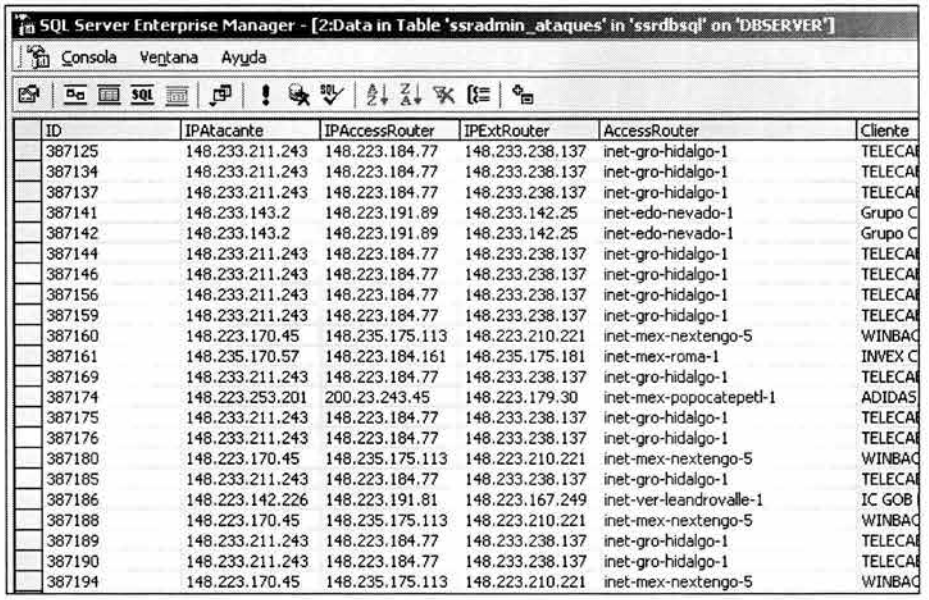


Figura 4.2.23 Ejecución de una consulta con el SQL Query Analyzer.



ID	IPAtacante	IPAccessRouter	IPExtRouter	AccessRouter	Cliente
387125	148.233.211.243	148.223.184.77	148.233.238.137	inet-gro-hidalgo-1	TELECAI
387134	148.233.211.243	148.223.184.77	148.233.238.137	inet-gro-hidalgo-1	TELECAI
387137	148.233.211.243	148.223.184.77	148.233.238.137	inet-gro-hidalgo-1	TELECAI
387141	148.233.143.2	148.223.191.89	148.233.142.25	inet-edo-nevado-1	Grupo C
387142	148.233.143.2	148.223.191.89	148.233.142.25	inet-edo-nevado-1	Grupo C
387144	148.233.211.243	148.223.184.77	148.233.238.137	inet-gro-hidalgo-1	TELECAI
387146	148.233.211.243	148.223.184.77	148.233.238.137	inet-gro-hidalgo-1	TELECAI
387156	148.233.211.243	148.223.184.77	148.233.238.137	inet-gro-hidalgo-1	TELECAI
387159	148.233.211.243	148.223.184.77	148.233.238.137	inet-gro-hidalgo-1	TELECAI
387160	148.223.170.45	148.235.175.113	148.223.210.221	inet-mex-nextengo-5	WINBAC
387161	148.235.170.57	148.223.184.161	148.235.175.181	inet-mex-roma-1	INVEX C
387169	148.233.211.243	148.223.184.77	148.233.238.137	inet-gro-hidalgo-1	TELECAI
387174	148.223.253.201	200.23.243.45	148.223.179.30	inet-mex-popocatepetl-1	ADIDAS
387175	148.233.211.243	148.223.184.77	148.233.238.137	inet-gro-hidalgo-1	TELECAI
387176	148.233.211.243	148.223.184.77	148.233.238.137	inet-gro-hidalgo-1	TELECAI
387180	148.223.170.45	148.235.175.113	148.223.210.221	inet-mex-nextengo-5	WINBAC
387185	148.233.211.243	148.223.184.77	148.233.238.137	inet-gro-hidalgo-1	TELECAI
387186	148.223.142.226	148.223.191.81	148.223.167.249	inet-ver-leandrovalle-1	IC GOB
387188	148.223.170.45	148.235.175.113	148.223.210.221	inet-mex-nextengo-5	WINBAC
387189	148.233.211.243	148.223.184.77	148.233.238.137	inet-gro-hidalgo-1	TELECAI
387190	148.233.211.243	148.223.184.77	148.233.238.137	inet-gro-hidalgo-1	TELECAI
387194	148.223.170.45	148.235.175.113	148.223.210.221	inet-mex-nextengo-5	WINBAC

Figura 4.2.24 Selección de todos los registros desde el Enterprise Manager.

Una vez creadas todas las tablas de la base de datos para el sistema, se procede a la configuración del servicio de WWW, el cual es realizado utilizando el **IIS** (Internet Information Server – Servidor de Información de Internet) que viene incluido en la instalación del Windows 2000 Server. Figura 4.2.25

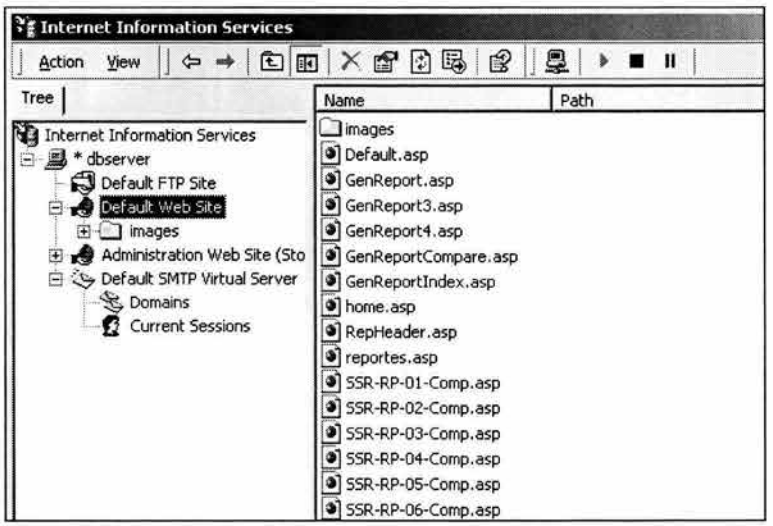


Figura 4.2.25 Configuración del servicio WWW en Windows 2000.

Para la configuración de este servicio, únicamente es necesario el desarrollo de las páginas y colocarlas en el directorio que establece por defecto el servicio de WWW en windows (C:\inetpub\wwwroot), y verificar que éste se encuentre ejecutándose mediante el uso de la consola de administración de servicios de internet mencionada anteriormente.

En la columna de la izquierda se ven los servicios que están configurados en el servidor, que son en este caso FTP, WWW y **SMTP** (Simple Mail Transfer Protocol – Protocolo de Transferencia de Correo Simple). Para verificar que un servicio se encuentre ejecutando, solamente se verifica que no aparezca la palabra '(Stopped)' o '(Detenido)' a un lado del nombre. Para el caso de la figura, el servicio de **Default Web Site** (Sitio Web Predeterminado) se encuentra ejecutándose y es el que se necesita para la parte WEB del sistema. A la derecha se observan las páginas ASP que forman parte del sitio WEB y que pueden ser consultadas desde cualquier cliente utilizando un navegador para internet.

Una vez terminado este proceso, se termina la configuración del Back-End y se procede a configurar el Front-End.

4.3 DISEÑO Y CONSTRUCCIÓN DEL FRONT-END

El Front-End está constituido por toda la parte de desarrollo de la aplicación y es lo que finalmente será ejecutado en las terminales de los operadores. El sistema y el ambiente de desarrollo se ejecuta en una computadora con el sistema operativo Windows XP. El desarrollo de la aplicación se lleva a cabo utilizando Microsoft Visual Basic 6.0 en su edición empresarial, y las herramientas de conectividad que maneja Windows XP para la conexión con el servidor de base de datos de Microsoft SQL Server 2000 que constituye la parte del Back-End. A través de las terminales de desarrollo son construidas también las páginas ASP necesarias para el despliegue de reportes de operación a través de una interfaz WEB, y las cuales serán depositadas para su uso en el servidor de Back-End.

Inicialmente, para la preparación del Front-End, se instala Visual Basic 6.0, el cual viene incluido en el grupo de herramientas de desarrollo de Microsoft Visual Studio 6.0.

Para la selección de los componentes de la instalación, se eligió la herramienta Visual Basic 6.0, así como todo el software de acceso a datos y controles ActiveX, también se instalaron algunos elementos de gráficos, como íconos e imágenes para darle al sistema la presentación visual que tienen las aplicaciones que se ejecutan bajo Windows.

En la figura 4.3.1 se demuestra la selección de los componentes de instalación en donde también es posible ver que se selecciona el Visual Interdev 6.0, que es una herramienta de edición de páginas WEB y es útil para el caso del desarrollo de las páginas ASP que forman parte del sistema.

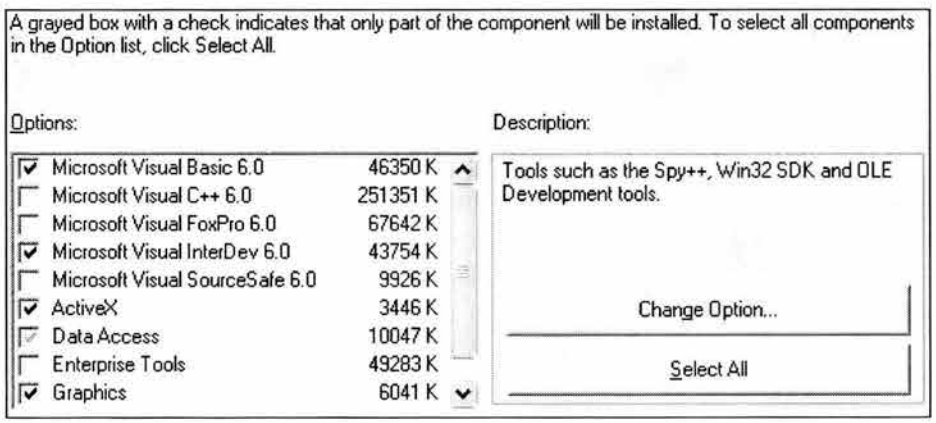


Figura 4.3.1 Selección de los componentes de la instalación

Posteriormente a la selección de los componentes se inicia la copia de archivos y el registro de los componentes instalados en el equipo. Al aparecer el mensaje de la figura 4.3.2, se termina la instalación y es posible empezar a utilizar el software para desarrollo de aplicaciones.

Figura 4.3.2 Finalización de la instalación de Visual Basic 6.0.

Antes de comenzar a desarrollar la aplicación, es necesaria la configuración de la conectividad a través de la red con el servidor de la base de datos de SQL, y para ello se tienen que realizar algunos procedimientos.

Es necesario acceder a las herramientas administrativas del sistema, las cuales se ubican como un elemento del Panel de Control de Windows XP, y seleccionar la opción Orígenes de Datos (ODBC), como en la figura 4.3.3 para abrir el diálogo de configuración de ODBC que se muestra en la figura 4.3.4.

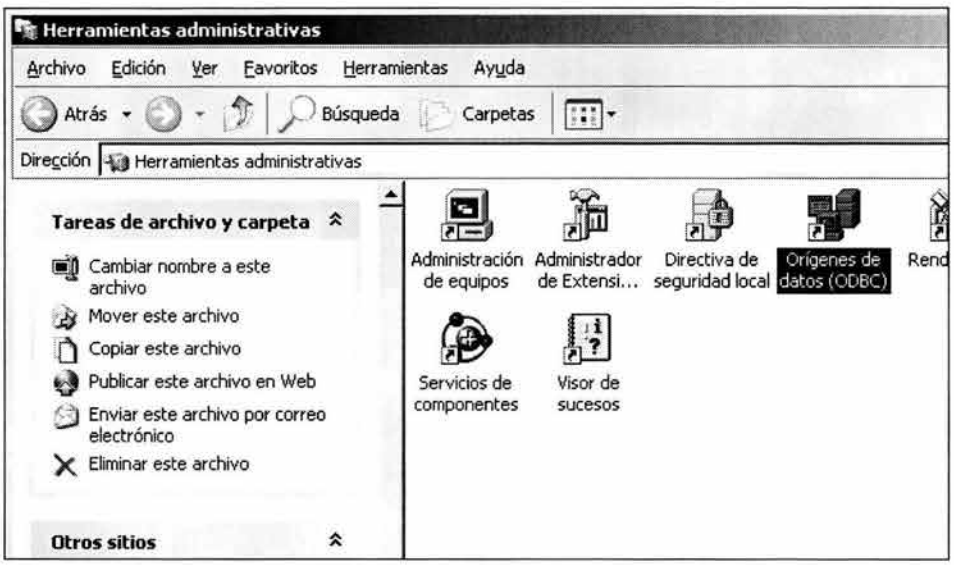


Figura 4.3.3 Herramientas administrativas de Windows XP

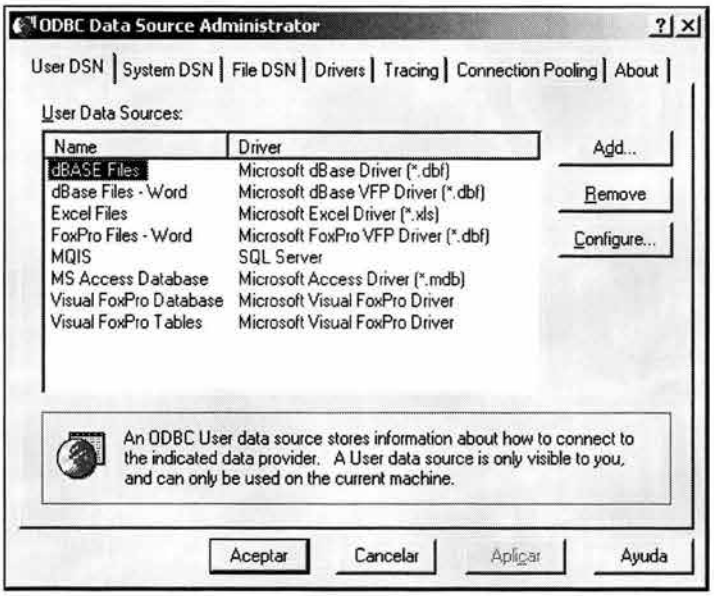


Figura 4.3.4. Configuración de origen de datos.

Al abrir el cuadro de diálogo se especifica un **DSN** (Data Source Name – Nombre de Origen de Datos) de sistema, el cual servirá como conector hacia el servidor de SQL, por lo que se debe seleccionar la ficha DSN del Sistema, como se ve en la figura 4.3.5.

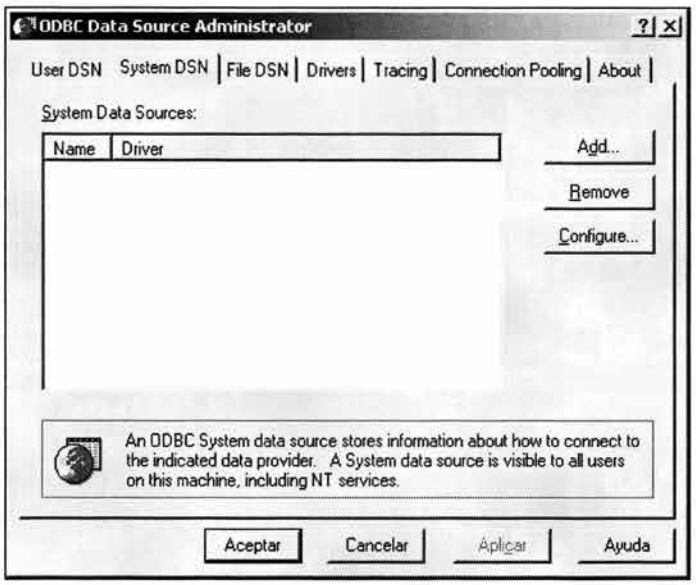


Figura 4.3.5 Selección de la ficha DSN del Sistema.

Cuando se selecciona la opción de agregar un nuevo DSN del sistema, aparecerá un nuevo cuadro de diálogo como el de la figura 4.3.6, y en el cual se especifica el tipo de base de datos al que se hará la conexión, que en este caso es de SQL Server.

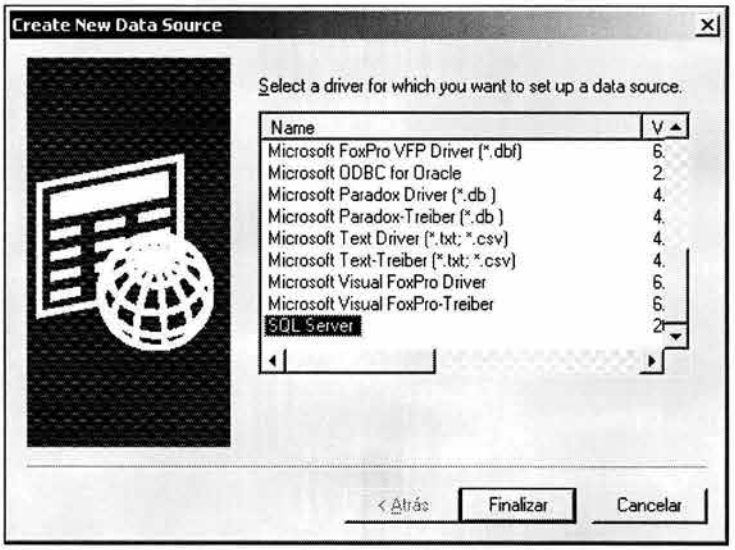


Figura 4.3.6 Selección de origen de datos para SQL Server.

Cuando se finaliza, aparece un asistente, en donde se especifican los parámetros de conexión con el servidor de SQL Server y que tienen que ver directamente con los parámetros de la instalación y configuración del Back-End. Estos son:

- Nombre del servidor de SQL Server, que en este caso es DBSERVER.
- Nombre de la base de datos, que en este caso es ssrdbsql
- Protocolo de conexión y puerto TCP, siendo para este caso por el puerto 1433 de TCP.
- Nombre de usuario y contraseña para conexión a base de datos, que en este caso es el usuario sa.

En la primera sección del asistente de configuración se especifica el nombre con el que se llamará al DSN, tomando en este caso el mismo nombre que el de la base de datos; la descripción del DSN y el servidor al cual se realizará la conexión. Estos parámetros se especifican en los campos como los que se muestran en la figura 4.3.7.

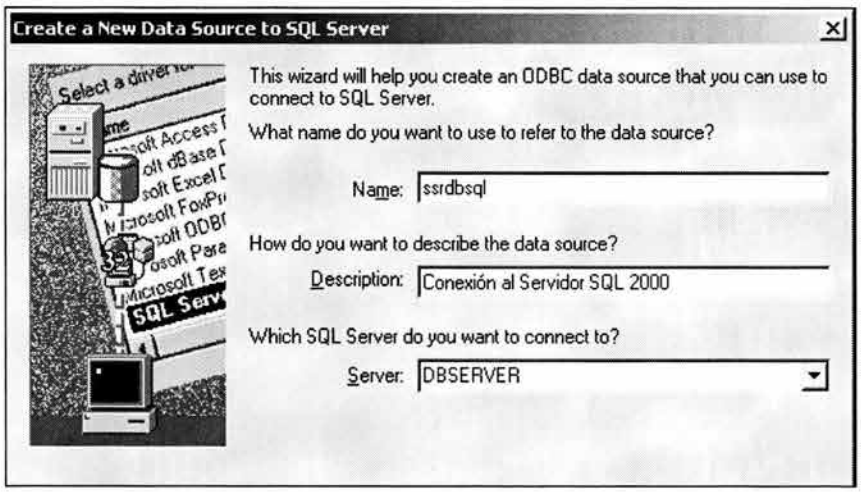


Figura 4.3.7 Especificación del nombre del DSN, descripción y servidor de SQL

Posteriormente se especifica el usuario para realizar la conexión, en la interfaz de la figura 4.3.8.

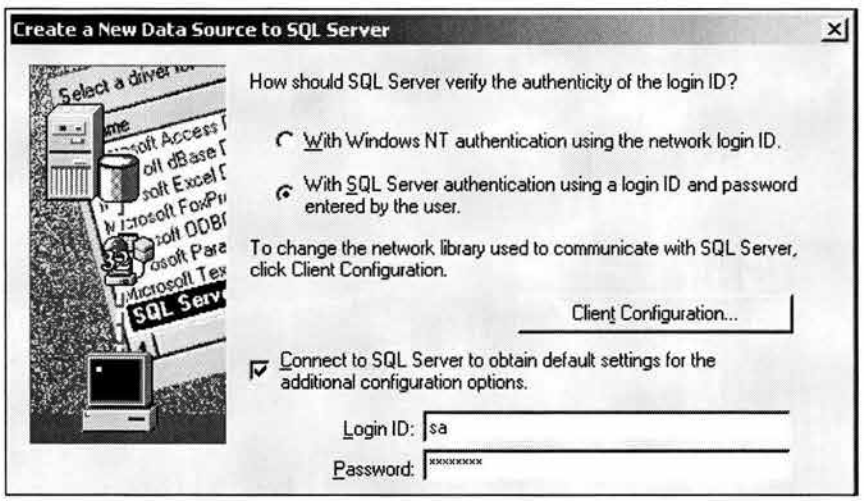


Figura 4.3.8 Especificación del usuario sa para la conexión al servidor SQL.

Al presionar el botón **Client Configuration** (Configuración del cliente) se muestra un diálogo como el de la figura 4.3.9, donde se especifica el protocolo de conexión y el puerto TCP.

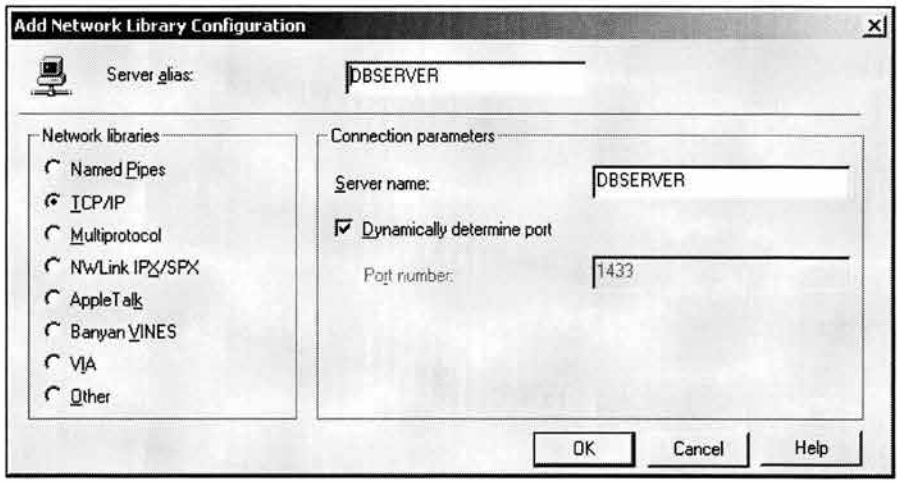


Figura 4.3.9 Especificación de parámetros de conexión.

Por último, la especificación de la base de datos a la que se va a acceder, se realiza en la sección del asistente mostrada en la figura 4.3.10. las demás opciones se dejan como las predeterminadas.

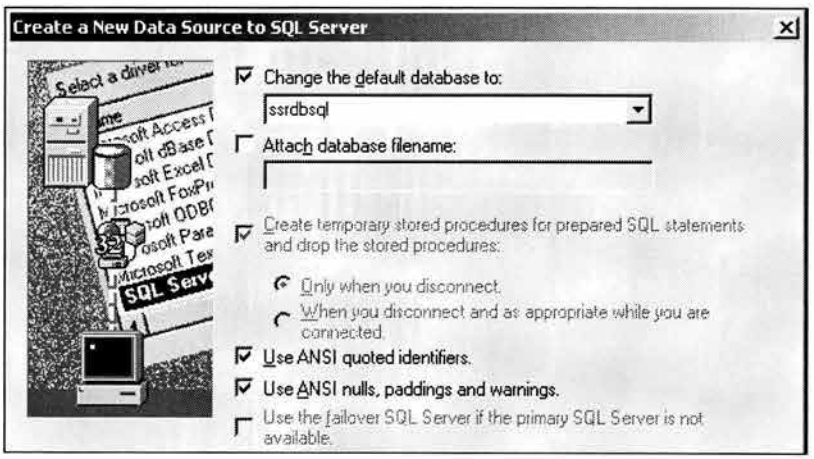


Figura 4.3.10 Especificación de la base de datos.

Posteriormente se procede a probar que la conexión se realice de manera exitosa, mediante una ventana que se muestra en las figuras 4.3.11 y 4.3.12. Al final de ellas se aceptan todos los cuadros de diálogo, quedando configurado en su totalidad el DSN.

Figura 4.3.11. Inicio de la prueba del DSN.

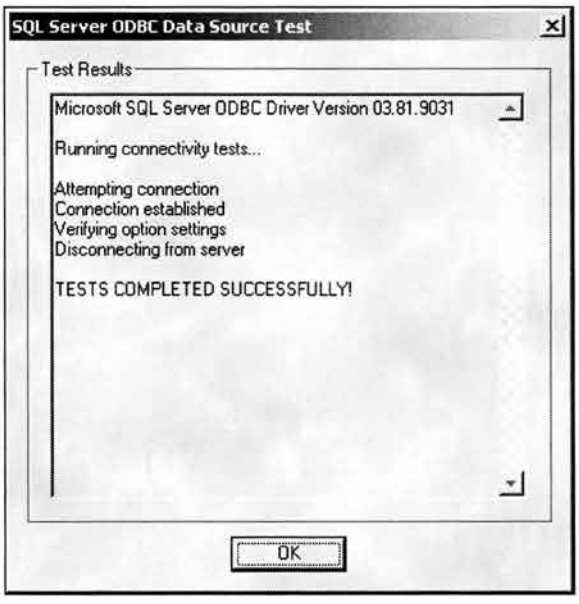


Figura 4.3.12 Verificación de prueba de conexión exitosa.

Una vez que se realiza la configuración de los orígenes de datos y que el Visual Basic 6.0 se encuentra instalado en el sistema, se procede a la generación y codificación de la aplicación.

Para ello tenemos las siguientes características técnicas generales a considerar para iniciar el nuevo proyecto en Visual Basic 6.0.

- El tipo de proyecto de Visual Basic es **Standard EXE** (Ejecutable Estándar), ya que se ejecuta directamente como aplicación de Windows.

- Las ventanas de la aplicación son independientes una de otra, es decir, se utiliza la opción de **SDI** (Single Document Interface – Interfaz de Documento Simple) para el tipo de aplicación.

- Contiene una ventana principal con una barra de menús y una barra de herramientas. Desde esta ventana son llamadas las demás de acuerdo a las opciones seleccionadas.

- El componente de Visual Basic 6.0 utilizado para la conexión con la base de datos SQL Server es el **ADO** 2.6 (ActiveX Data Objects – Objetos de Datos ActiveX).

- Se utiliza el objeto de datos **DAO** (Data Access Objects – Objetos de Acceso a Datos) para el uso de una base de datos temporal en Access para el módulo de generación de bitácoras de operación de red.

- Se utilizan consultas SQL realizadas desde la aplicación y no como procedimientos almacenados o vistas, debido a que no presentan una muy alta complejidad.

- Se utiliza el componente **HTML Object Library** (Librería de Objetos HTML) para la generación de los reportes.

- Los reportes se generan mediante la ejecución de páginas ASP, que hacen uso de ADO desde el servidor para la conexión con SQL, debido a que son ejecutadas en él, y solo el HTML resultante es mostrado en los navegadores de las terminales.

- Se genera un módulo exclusivo para la codificación de funciones, variables y constantes que son llamadas desde cualquier forma que constituye la aplicación.

Para la construcción de la interfaz de usuario del sistema, se construyeron varias formas de Visual Basic, utilizando los principales controles existentes en una ventana de windows.

- Ventanas.
- Botones.
- Cuadros de texto.
- Listas desplegables.
- Barras de herramientas.
- Menús.
- Cuadros de verificación y radio botones.

Para iniciar el desarrollo del sistema, se inicia Visual Basic 6.0. En la figura 4.3.13, se presenta el inicio del proyecto, indicándole al ambiente de desarrollo de Visual Basic 6.0 que se tratará de un ejecutable estándar de Windows.

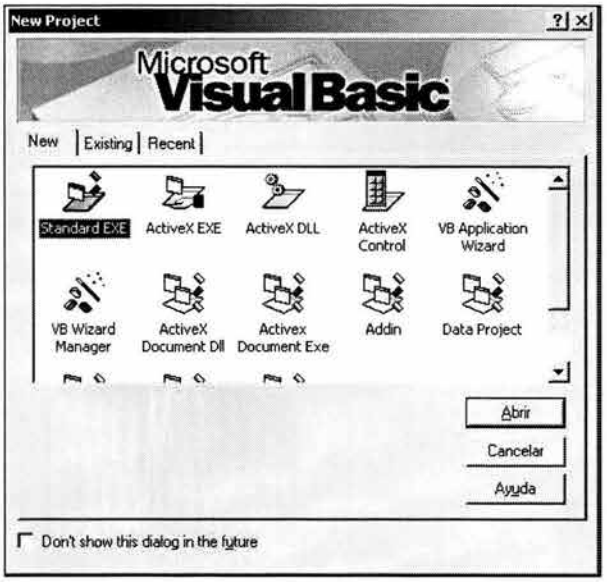


Figura 4.3.13. Inicio del proyecto.

La forma inicial para el ingreso al sistema consta de un cuadro de diálogo en donde el operador deber introducir el usuario Administrador y su contraseña. El diseño de esta forma se muestra en la figura 4.3.14, en el cual se puede observar el uso de los controles estándar de Windows desde el inicio del proyecto, y los cuales se van utilizando a lo largo de todas las formas que lo constituyen.

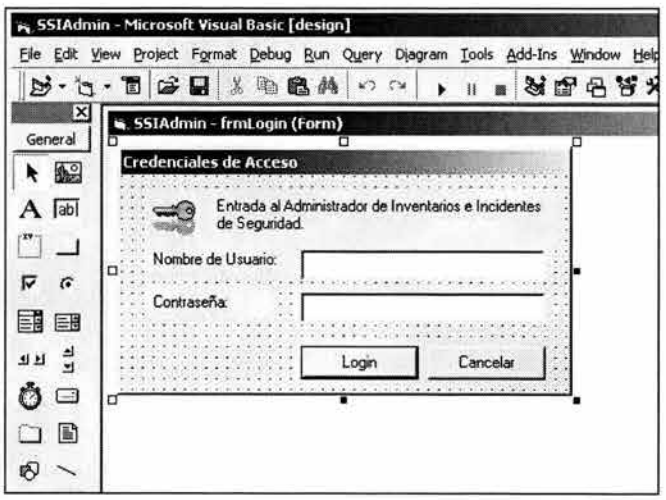


Figura 4.3.14 Diseño de la forma inicial del sistema.

Del lado izquierdo de la ventana del ambiente de desarrollo de Visual Basic, se presenta la caja de herramientas, de la cual se van tomando los controles que se insertan en las formas. Del lado derecho, se tiene el explorador, que indica todos los elementos, como formas y módulos que constituyen el proyecto; la sección de propiedades del control que actualmente se encuentra seleccionado en la forma en que se está trabajando y el mapa de ubicación de la forma actual en el escritorio de Windows.

Para insertar los controles en la forma que se está desarrollando, simplemente se deben seleccionar el deseado de la barra de herramientas y dibujarlo sobre ella, estableciendo de esta forma el tamaño, las propiedades del objeto y el código asociado. Este último se escribe cuando se hace doble clic sobre el control de que se trate y se abre la ventana de código correspondiente a cada uno de los eventos que el control lleva asociado. El primer evento que abre es el predeterminado, por ejemplo, para un botón, el evento predeterminado es el "clic" sobre él. El proceso de arrastre de controles para la forma inicial se muestra en la figura 4.3.15

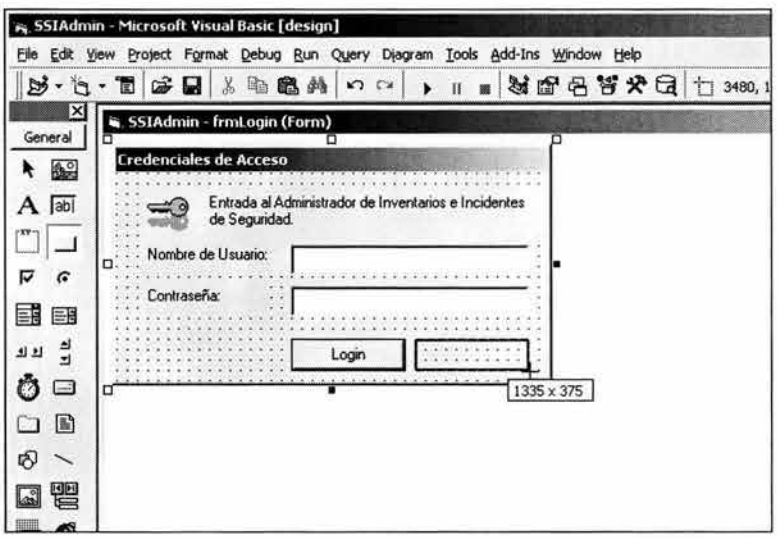


Figura 4.3.15 Colocación de los controles sobre la forma.

A cada control que se inserta en una forma se le asignan propiedades, las cuales se refieren principalmente a su nombre, su tamaño, su ubicación dentro de la forma, el tipo de letra de la leyenda o leyendas que incluyen, la propia leyenda, si son de solo lectura para el caso de cajas de texto, el estilo, entre otros. Estas características definirán al objeto y dependerán de la apariencia que se le desee dar y la funcionalidad que tendrá. La figura 4.3.16 muestra la edición de propiedades de un botón.

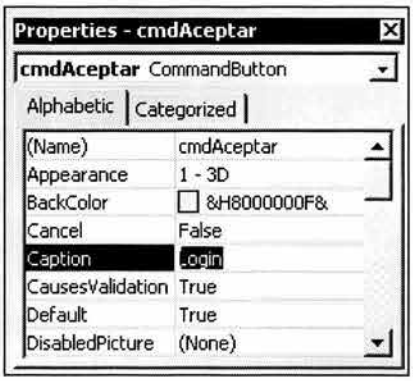


Figura 4.3.16 Asignación de propiedades de un control.

La ventana principal de la interfaz de usuario del sistema, es la mostrada en la figura 4.3.17, en la que se observa su diseño, y en donde se utilizan controles comunes de Windows como barra de menús, barra de herramientas, listas tipo árbol, listas, barra de estado, y otros que no son visibles en la ejecución como tales, sino que se utilizados como parte de otros controles, como el caso de las listas de imágenes.

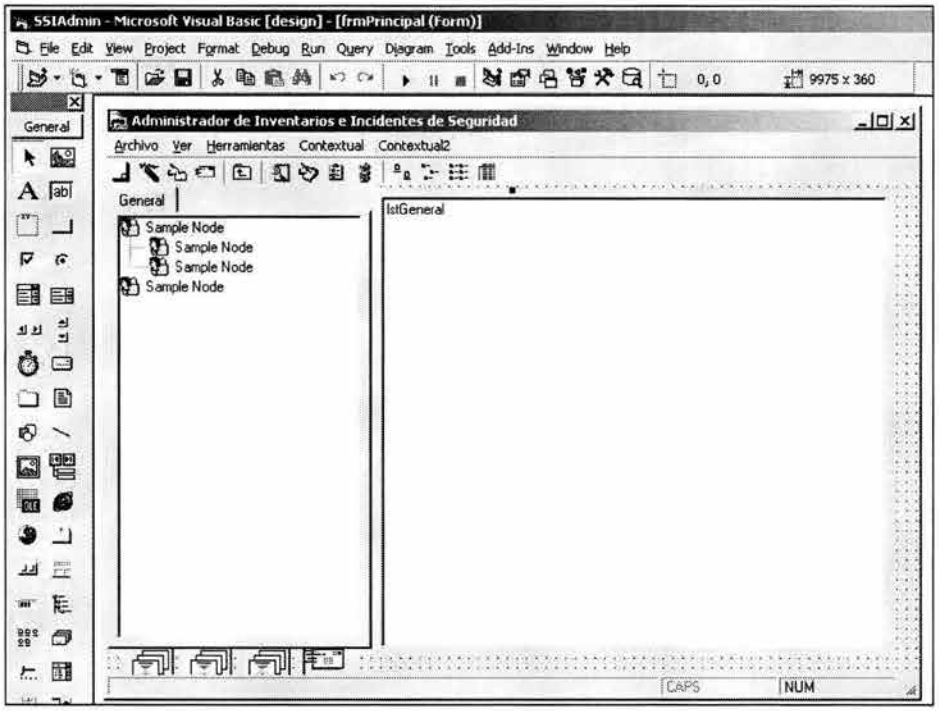


Figura 4.3.17 Diseño de la ventana principal del sistema.

Los controles que constituyen esta forma desempeñan cierta función dentro del sistema, y son mencionados a continuación.

- La barra de menú, en donde se encuentra la llamada a todas las funcionalidades del sistema, mediante la apertura de nuevas ventanas y controles.

- Barra de herramientas se incluyen las opciones más importantes y de uso frecuente de las incluidas en el menú principal.

- La lista tipo árbol, del lado izquierdo, en la cual se muestran los elementos de información del sistema, y que a su vez contienen otros elementos. Por ejemplo, las categorías de usuarios, que contienen perfiles de usuarios, y que a su vez contienen usuarios.

- La lista, del lado derecho, en donde se despliegan los elementos contenidos en algún nodo del árbol.

- La barra de estado, donde se muestran descripciones o comentarios de los elementos seleccionados en la lista, así como el estado de las teclas de bloqueo numérico y de mayúsculas.

- Controles no visibles, como las listas de imágenes y de las cuales se toma su contenido para incluirlo en las barras de herramientas o íconos mostrados en la lista y el árbol; y control de correo o SMTP, que es utilizado para la llamada a sus métodos en el caso del envío de notificaciones. Estos controles no se ven en la ejecución del proyecto.

Toda la información que se presenta en el árbol y en la lista, es obtenida de la base de datos de SQL Server, y éstos se van llenando una vez que se hizo una consulta de los datos partiendo de tres categorías de operación de la forma principal del sistema: administración de usuarios, administración de equipos y notificaciones.

Para la administración de equipos, se hace una consulta en donde se obtienen los datos correspondientes de los equipos de red, de acuerdo a la plataforma donde son incluidos.

Lo anterior es aplicado de igual forma para la administración de usuarios, en donde, para este caso se consideran las categorías o plataformas, los perfiles y los usuarios incluidos dentro de ellos.

Entonces, para generar los nodos del árbol del lado derecho, se consideran los objetos que no son terminales, es decir, todos aquellos que contienen otros elementos. Por ejemplo, la categoría de usuarios, los grupos o perfiles, las plataformas de equipos y el grupo de notificaciones son elementos no terminales que durante la ejecución del sistema serán mostrados del lado izquierdo, en el árbol. Para la generación de los

elementos de la lista del lado derecho de la ventana, basta con hacer clic sobre un nodo del árbol cuando el programa se está ejecutando, y a continuación todas las ramas que parten de él directamente son mostradas. El funcionamiento es similar al que presenta el explorador de archivos de Windows.

De acuerdo a la información que es desplegada en la lista de la derecha, se habilitan o deshabilitan los botones de la barra de herramientas que permitan ejecutar ciertas acciones sobre los elementos mostrados, así como también se agregan los campos que serán mostrados de acuerdo al elemento que se seleccionó en el árbol.

En la figura 4.3.18, se presenta el diseño para la forma de edición para la información de un usuario, y en la cual se muestran los campos de captura. Esta forma es utilizada tanto para agregar un nuevo usuario como para la modificación de la información de uno ya existente.

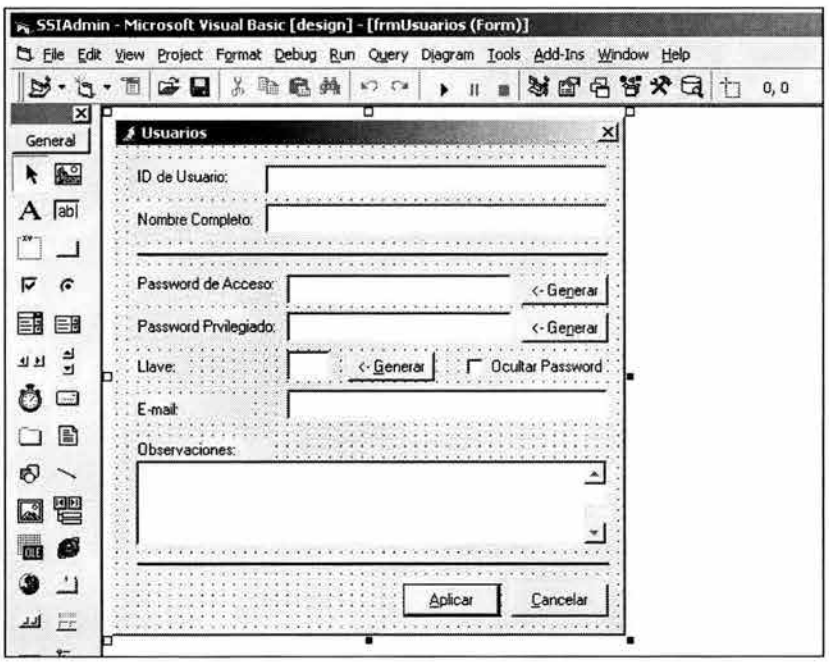


Figura 4.3.18 Diseño de la forma para edición de información de usuarios.

De acuerdo a la opción seleccionada, que en este caso puede ser el alta de un usuario nuevo en el sistema, o bien, la actualización de datos de un usuario ya existente, se realiza la operación correspondiente en la base de datos y que para estos casos se trata de una sentencia INSERT para insertar un nuevo registro, o una sentencia UPDATE para la actualización.

El proceso que se realiza para la consulta, edición o alta de un usuario es similar para el caso de equipos de red y notificaciones, en donde se utilizan las mismas sentencias de SQL mencionadas anteriormente con sus parámetros correspondientes y que son llamados desde el código de la aplicación.

La figura 4.3.19 es el diseño para la edición de equipos de red.

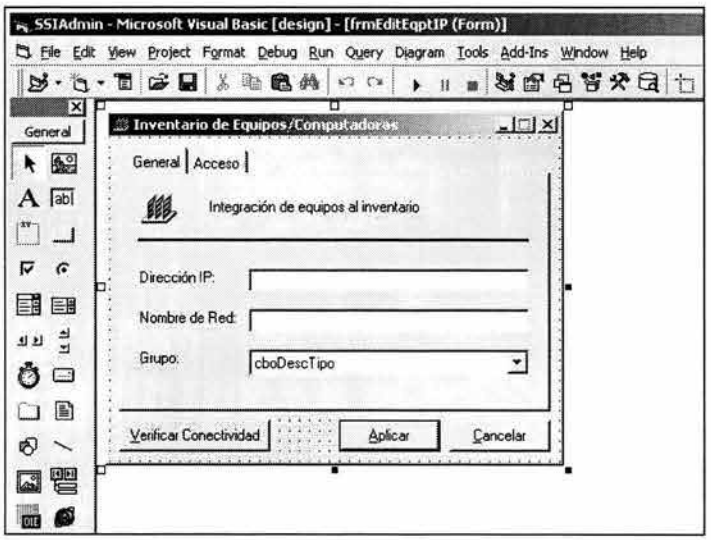


Figura 4.3.19 Diseño de la forma de edición de equipos de red.

Para la administración de incidentes de seguridad, se manejan conceptos similares para el alta, sin embargo esta también dependerá de la existencia de un incidente proveniente de la misma dirección IP con anterioridad, ya que en caso de existir mostrará el contenido de los datos ya capturados en los campos correspondientes, con excepción de la fecha y tipo de incidente.

El diseño de la ventana de captura de incidentes está en las figuras 4.3.20 y 4.3.21, y está dividida en dos secciones, cada sección separada en una pestaña diferente, la primera consiste en la información del incidente y los datos de acceso hacia la dirección IP involucrada, y la segunda los datos de responsable y contacto técnico. En el campo de comentarios se llena con la información de seguimiento del incidente, y donde el operador anotará sus avances en la actividad.

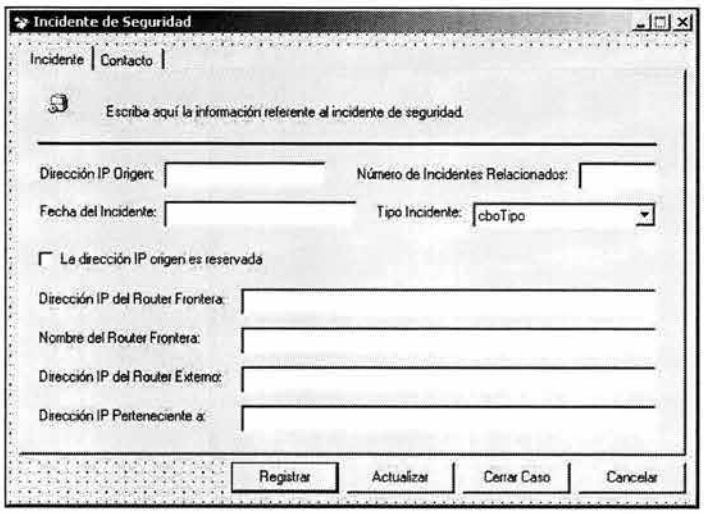


Figura 4.3.20 Diseño de forma de captura de incidentes: datos generales.

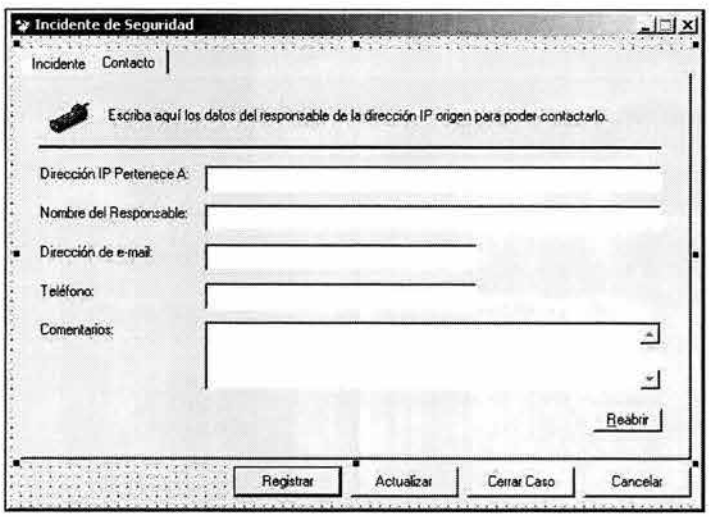


Figura 4.3.21 Diseño de la forma de captura de incidentes: datos de contacto.

Cuando se captura el campo 'Dirección IP origen' se realiza una búsqueda de la dirección especificada, para verificar casos anteriores. En caso de no existir información anterior se procede a la captura de todos los campos y si ya se cuenta con información, se llena el contenido de dichos campos con la información obtenida de la base de datos. Cuando el operador escribe la IP origen y presiona la tecla de tabulador para pasar al siguiente campo, se ejecuta el proceso, por lo que puede observarse que esta acción de búsqueda se ejecuta en base a un evento. Este evento es el de pérdida de foco en el campo IP origen, es decir, que el cursor pase de ese a otro campo.

El registro de los datos capturados a la tabla de incidentes también se realiza mediante la sentencia INSERT de SQL, mientras que la actualización de la información de alguno mediante la sentencia UPDATE.

Para que la aplicación sea visualizada como parte de Windows, se crearon algunas formas que incluyen barras de progreso y porcentajes y mediante las cuales el personal que opera el sistema podrá ver el avance de una actividad realizada por la aplicación, por ejemplo, en el envío de notificaciones, y en la cual se podrá observar dicha barra hasta la finalización de la acción. En la figura 4.3.22 se encuentra el diseño de una forma de este tipo.

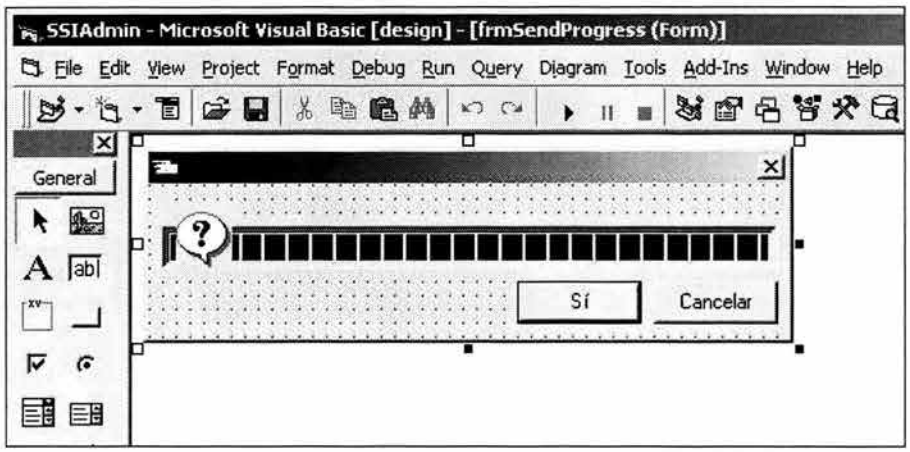


Figura 4.3.22 Diseño de forma para mostrar el progreso de envío de notificaciones.

La sección de búsquedas tiene la finalidad de ofrecer al operador una manera fácil y rápida de localizar un elemento dentro del sistema, por ejemplo, si es necesario localizar a qué grupo pertenece cierto usuario y de que plataforma se trata, lo podrá realizar mediante la utilización de este módulo. La operación de esta sección de la aplicación está basada principalmente en el uso de sentencias SELECT de SQL a través de todas las tablas que contienen información referente a un rubro en particular, además de hacer la búsqueda tomando en cuenta no solamente un campo sino varios, dependiendo el tipo de búsqueda de que se trate, por ejemplo, para buscar un equipo integrado, no solo se podrá hacer mediante solamente la IP o solo el nombre, sino por cualquiera de ambos datos. La construcción de la forma de búsquedas se presenta en la figura 4.3.23 y está dividida en búsqueda de usuarios, de equipos o de incidentes de seguridad.

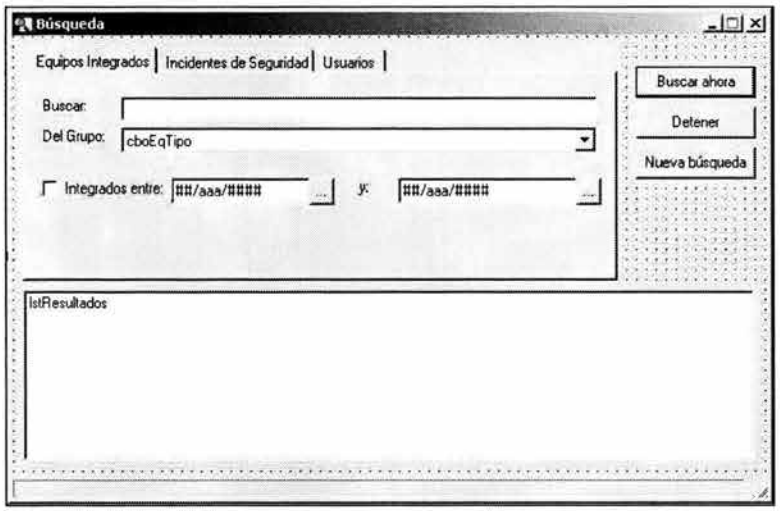


Figura 4.3.23 Diseño de la ventana de búsquedas.

Para la sección de reportes se utiliza una ventana que contiene un control para despliegue de páginas WEB. Esta forma es llamada una vez que se realiza la solicitud de número de reporte y las fechas de consulta. Para la codificación de los reportes se utiliza ASP y HTML, para verlos como contenido WEB, y se realiza utilizando una editor llamado Visual Interdev incluido en el Visual Studio. El diseño de la ventana del sistema donde se consultan los reportes se muestra en la figura 4.3.24.

Todas las páginas ASP son depositadas en el servidor, para que cualquier terminal pueda hacer uso de ellas. Cuando se solicita un reporte, una vez tomada la información necesaria, se llaman estas páginas, pasándoles como parámetro esta información.

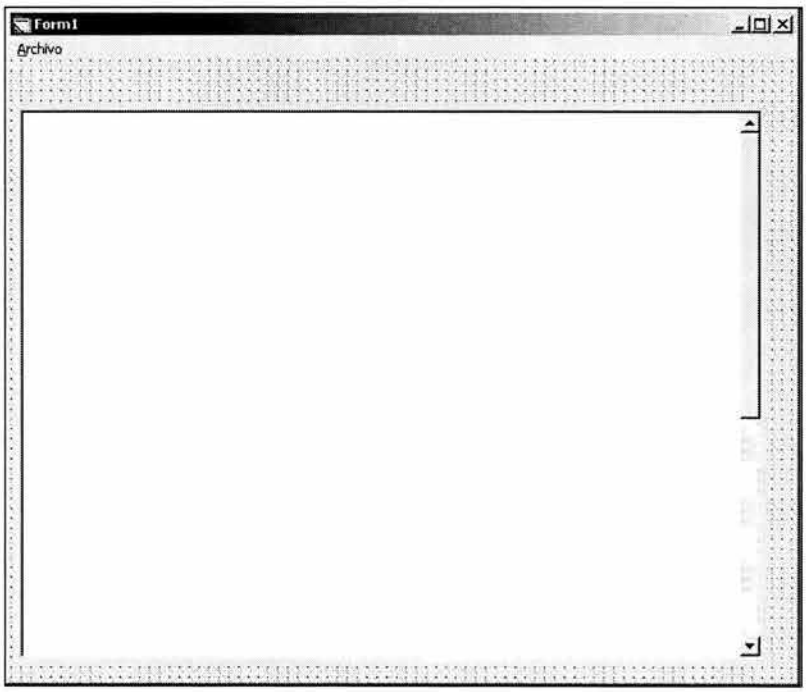


Figura 4.3.24 Diseño de la ventana de reportes.

Para la distribución de la aplicación a las diferentes terminales, es necesario la generación de un archivo ejecutable de Windows que sea instalado en cada una de ellas. Cuando se genera el paquete de instalación se incluyen también todas las librerías y controles necesarios para que se ejecute exitosamente la aplicación, mediante un asistente llamado **Package & Deployment Wizard** (Asistente para paquetes y distribución de aplicaciones).

Al especificar el proyecto que se va a distribuir y seleccionando la opción **Package** (Paquete), se genera un instalador llamado setup.exe, que deberá ser ejecutado en todas las terminales que usarán el sistema, de esta manera no es necesario que cada terminal tenga instalado Visual Basic para ejecutar la aplicación.

4.4 PRUEBAS E IMPLANTACIÓN DEL SISTEMA

Para que el sistema comience a operar de manera adecuada, tiene que ser probado utilizando diferentes tipos de pruebas.

- Pruebas de caja negra. Las pruebas de caja negra se realizan mediante la ejecución del programa, orientándolas principalmente a la especificación y no a la observación del código. Las partes principales de esta prueba son las entradas y las salidas. Estas pruebas pueden ser realizadas por el usuario final de la aplicación.

- Pruebas de caja blanca. Las pruebas de caja blanca son realizadas con el conocimiento del código que constituye el sistema, así como todo su funcionamiento. Este tipo de pruebas se realizan por los programadores únicamente. En este método se incluyen pruebas de instrucciones, pruebas de decisiones y pruebas de ciclos.

- Pruebas de integración Top-Down. Es un método incremental para construir las estructura del sistema. Los módulos son integrados hacia abajo, empezando por el módulo principal. Los módulos que son subordinados de los módulos de control se incorporan al sistema a manera de ramas o por niveles.

- Pruebas de integración Bottom-Down. Esta prueba empieza desde los módulos de trabajo y continúa hacia arriba. Por su naturaleza es necesario que los módulos de trabajo estén terminados antes que los de control.

- Pruebas de regresión. Aunque el sistema puede ser probado completamente durante su desarrollo para satisfacer un requerimiento determinado, el programa puede cambiar durante el mantenimiento y se requiere que todas las partes sean probadas nuevamente. Este proceso valida las partes modificadas, asegurando que éstas no provoquen errores en las partes ya probadas con anterioridad. En las

pruebas de regresión, a diferencia de las pruebas durante el desarrollo, un conjunto establecido de pruebas pueden ser reutilizadas.

- Pruebas de volumen. En este tipo de pruebas se hace una simulación del uso de la aplicación por varios usuarios y numerosos datos, midiendo el rendimiento de los diversos fragmentos de código y extrayendo información útil para su optimización.

Dentro del proceso de desarrollo e implementación del sistema se contempló un periodo de pruebas.

Probar es el proceso de ejecutar el sistema con la intención de encontrar errores. Para probarlo necesitamos una serie de datos, los datos de entrada (input). Para saber si existe un error o no, entonces también fue necesario saber las salida esperada (output), así como el método a utilizar.

El método de pruebas que se utilizaron para el sistema de inventarios constó de las pruebas de caja negra y las pruebas de caja blanca.

Pruebas de caja negra

En las pruebas de caja negra utilizamos todos los módulos para la verificación de factores como validaciones y análisis de valores frontera.

Pruebas de validación de direcciones IP

En el módulo de inventario de equipos se almacena la dirección IP del mismo, la cual es capturada por el operador teniendo que ser válida, con el conocimiento de que una dirección IP consta de 8 octetos de bits (o números decimales entre 0 y 255 solamente), no permitiendo escribir direcciones IP como 148.223.126.299, debido a que uno de los octetos es mayor a 255.

Sin la existencia de la validación correspondiente, la escritura de una dirección IP inválida, provoca almacenar información errónea en la base de datos. Al escribirla y verificar la conectividad al equipo, se recibe un error de sistema indicando que dicha IP no existe, como se ve en la figura 4.4.1.

Figura 4.4.1 Error de sistema sin validación de la dirección IP.

Para evitar este tipo de errores, y garantizar que la información almacenada en la base de datos es correcta, se incluyó un procedimiento de verificación de error en direcciones IP, el cual es disparado al momento de verificar la conectividad o intentar almacenar la información en la base de datos, mostrándole al operador un mensaje indicándole que la dirección IP no es válida.

Prueba de validación de fechas

En algunos módulos del sistema, es posible la introducción de fechas como entrada por parte del operador, para obtener, por ejemplo, un reporte o una búsqueda. Es importante no permitir la introducción de una fecha que no exista.

Cuando se inicia una búsqueda indicando una fecha inválida, el sistema envía un error como el de la figura 4.4.2, y terminando la ejecución de la aplicación.

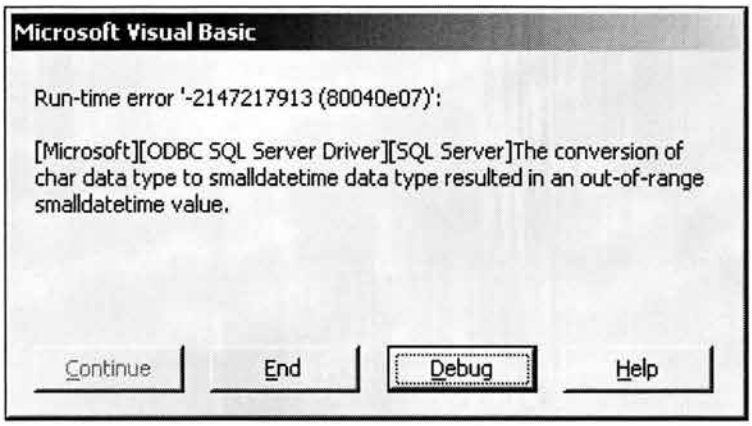


Figura 4.4.2 Error de sistema por fechas inválidas

Para darle solución, se incluye un módulo que no permite que el usuario escriba las fechas directamente en la ventana de la aplicación, sino que mejor las seleccione, como se ve en la figura 4.4.3.

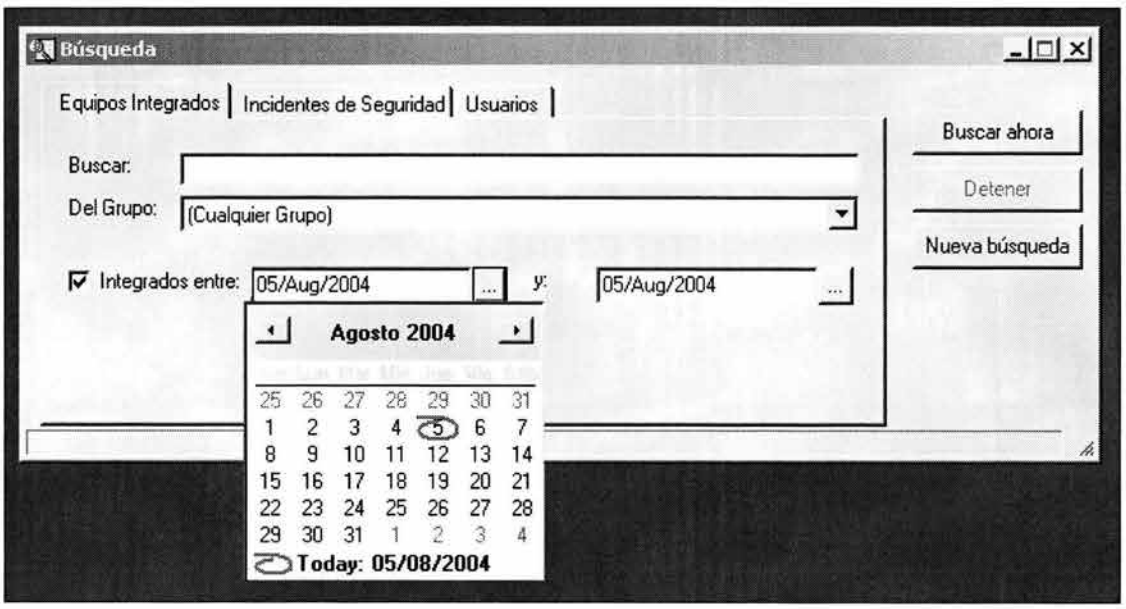


Figura 4.4.3 Validación de fechas

De esta manera se obtiene el resultado de la búsqueda de forma correcta.

Pruebas de caja blanca

En estas pruebas se revisó el código de cada una de los módulos de la aplicación para verificar que todas las instrucciones fueran ejecutadas. La figura 4.4.4 muestra la forma en que las condiciones deben ser cumplidas para que dependiendo de la elegida ejecute las instrucciones que debe.

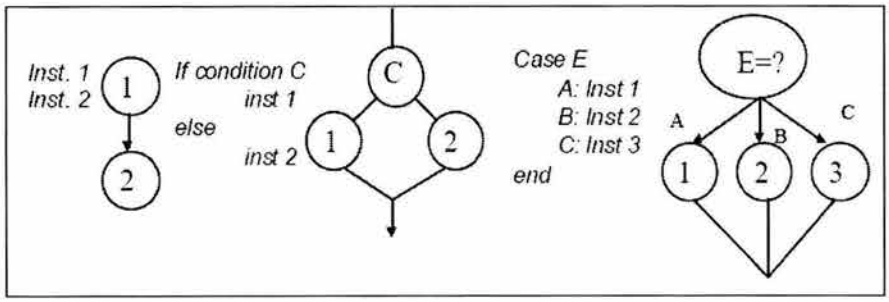


Figura 4.4.4 Pruebas de caja blanca.

Instrucciones secuenciales

A lo largo de todo el código existen instrucciones secuenciales que deben ser ejecutadas para la funcionalidad completa del sistema y cubrir las necesidades de toda la aplicación en su conjunto.

- Para acceder al sistema.
- Para integrar un equipo.
- Para dar de alta un usuario.
- Para registrar un incidente de seguridad
- Para dar de baja un equipo

- Para dar de baja un usuario
- Para hacer una búsqueda
- Para enviar una notificación
- Para cerrar un caso de incidente.
- Para salir del sistema

Dentro de estas funcionalidades del sistema existen condiciones simples y dobles, o bien múltiples que permitan decidir qué operación será realizada de acuerdo a la petición del usuario.

Condiciones dobles

Cuando se va a dar de baja un equipo, se cuestiona al usuario sobre la operación que va a realizar, y dependiendo de su respuesta, se ejecuta una acción. En la figura 4.4.5 el usuario decide entre contestar Si o No.

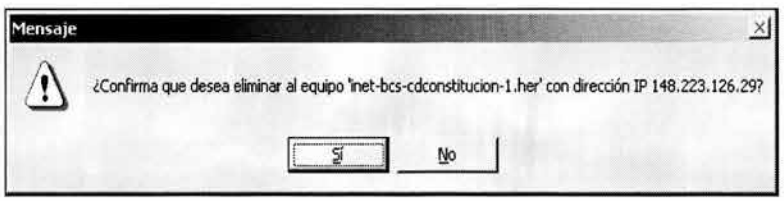


Figura 4.4.5 Condición doble

Condiciones múltiples

Para el módulo de búsquedas, se tienen 3 opciones: búsqueda de equipos integrados, búsqueda de usuarios y búsqueda de incidentes de seguridad. Para cada una se

ejecutarán una serie de instrucciones diferentes al presionar el botón de 'Buscar ahora'. La figura 4.4.6, muestra el resultado para una búsqueda de equipos integrados.

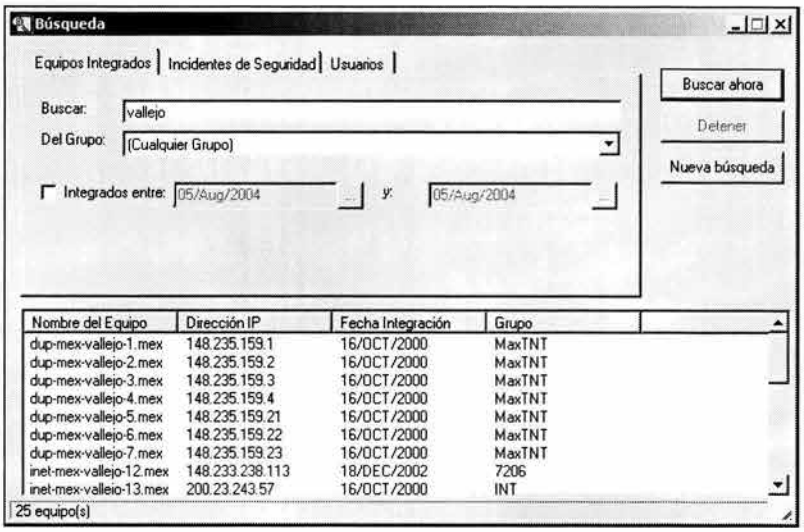


Figura 4.4.6 Búsqueda de equipos en el inventario

El sistema es capaz de verificar la opción seleccionada en la ventana antes de hacer la búsqueda y una vez presionado el botón 'Buscar ahora', tomar la ruta correcta y buscar en las tablas correspondientes.

Pruebas de regresión

En las pruebas de regresión del sistema se verifica que los diferentes módulos al ser agregados o modificados, no afecten la operación de los ya existentes. En este caso para la integración de nuevos equipos se obtiene un resultado al introducir a la base de datos la información de ellos. Al desarrollar el módulo de búsqueda de equipos, se pueden introducir datos de entrada como es la información de un equipo existente y obtener el resultado de la búsqueda sin interferir en la operación del módulo de integraciones.

Tipos de Mantenimiento

Un aspecto importante en el diseño y desarrollo de sistemas es el mantenimiento. Una vez acabada la fase de desarrollo y la implantación del sistema, es imprescindible garantizar el mantenimiento del mismo. Los programas deben ser modificados con el tiempo ya que las reglas de negocio pueden variar o es necesario adaptarse al entorno o a los cambios en los sistemas tecnológicos. Existen diferentes tipos de mantenimiento aplicables al sistema.

- Mantenimiento preventivo. Es la actividad en la cual se realizan cambios a la aplicación para mejorar el mantenimiento futuro, la estabilidad y confiabilidad en la operación. También es útil para proporcionar bases seguras sobre las que podrán implementarse mejoras posteriores.

- Mantenimiento correctivo. Se presenta cuando ocurre un error en la operación del sistema. Frecuentemente se cambia la implementación, de tal manera que las especificaciones se utilizan para verificar que la nueva implementación corrige los errores que se presentaron.

- Mantenimiento adaptativo. Se presenta cuando se generan cambios en los requerimientos de tal manera que la especificación sea adaptada a estos nuevos requerimientos y verificando que la nueva implementación cumpla con ellos. Estos requerimientos también pueden ser cambios en las plataformas de hardware o sistemas operativos.

- Mantenimiento perfectivo. Se realiza cuando existe la necesidad de optimización de procesos, sin que cambien forzosamente los requerimientos. La especificación permite entender claramente el impacto de los cambios de manera que éstos se implanten confiadamente.

4.5 FACTIBILIDAD TÉCNICA Y OPERATIVA

Factibilidad Técnica

El estudio de factibilidad técnica se basó en la evaluación del equipo con el que el departamento de seguridad de la empresa cuenta, así como las herramientas de software necesarias para que pueda desarrollarse un sistema que controle el inventario de usuarios, equipos y seguimiento de incidentes de seguridad, basándose en una arquitectura cliente-servidor, utilizando Microsoft Visual Basic 6.0 para el desarrollo de la parte cliente, y de Microsoft SQL Server 2000 para la parte servidor.

Actualmente la empresa cuenta con licencias disponibles para la instalación de SQL Server 2000 edición estándar, al igual que para la instalación de herramientas de desarrollo de aplicaciones en Visual Studio 6.0.

En la tabla 4.5.1 se presentan los requerimientos necesarios para que SQL Server 2000 edición estándar pueda ejecutarse.

Procesador	Procesador de la familia Pentium con 133Mhz de velocidad o mayor.
Sistema Operativo	• Windows Server 2003, Standard Edition, Enterprise Edition o Datacenter Edition. • Windows® 2000 Server, Advanced Server o Datacenter Server. • Windows NT® Server version 4.0 Standard o Enterprise Edition with Service Pack 5 (SP5) o mayor.
Memoria RAM	64 MB
Espacio en Disco Duro	270 MB
Unidades	CD-ROM

Tabla 4.5.1 Requerimientos para Microsoft SQL Server 2000.

En la tabla 4.5.2 se presentan los requerimientos necesarios para que Visual Basic 6.0 pueda ejecutarse en las terminales de desarrollo.

Procesador	Procesador de la familia Pentium con 90Mhz de velocidad o mayor.
Sistema Operativo	Windows 95 ó mayor.
Memoria RAM	32 MB
Espacio en Disco Duro	135 MB
Unidades	CD-ROM

Tabla 4.5.2 Requerimientos para Visual Basic 6.0

Para la operación óptima del sistema y la base de datos, se deben cubrir los requerimientos en un nivel mayor al mínimo requerido por los elementos y herramientas de software que servirán de soporte y plataforma de desarrollo para el sistema de administración de inventario de usuarios, equipos e incidentes de seguridad.

El equipo con que cuenta el departamento de seguridad para asignarlo como servidor de SQL 2000, cuenta con las siguientes características.

- Procesador Pentium 4 a 2.4 GHz.
- Sistema Operativo Windows 2000 Server
- Memoria RAM de 512 MB
- Disco Duro de 20 GB, con 12 GB de espacio libre.
- Unidad de CD-ROM

El sistema será operado en diez terminales que tendrán conexión con el servidor por medio de TCP/IP. Estas terminales cuentan con las siguientes características de hardware.

- Procesador Pentium 3 a 800 Mhz.
- Sistema Operativo Windows XP Profesional
- Memoria RAM de 256 MB
- Disco Duro de 15 GB, con 8 GB de espacio libre.
- Unidad de CD-ROM
- Gráficos Super VGA.

Se cuenta con personal con conocimientos necesarios de administración de SQL Server 2000 y Windows 2000, así como el personal necesario para el mantenimiento de la aplicación y atención a nuevos requerimientos y adecuaciones del mismo.

Factibilidad Operativa

El sistema será utilizado por la totalidad del personal del departamento de seguridad de la empresa, el cual consta de diez administradores, que harán conexiones simultáneas a un servidor con la información centralizada.

La operación del sistema deberá satisfacer los siguientes puntos en su operación.

- Desempeño. De acuerdo a las plataformas de hardware sobre las que se instalará el sistema, el rendimiento será adecuado, tomando en cuenta que el volumen de la información es adecuado a los recursos con los que cuenta el servidor.

- Información. Permitirá tener un recurso centralizado donde toda esta información sea almacenada, y podrá ser consultada y actualizada por todos los administradores que operen el sistema, afectando solo una fuente de datos.

- Economía. Debido a la existencia de licencias para el software empleado, al igual que de personal que tiene los conocimientos sobre las herramientas, se espera contar con tiempos de atención cortos, además de no requerir personal adicional.

- Control. Toda la información del departamento de seguridad estará almacenada en una base de datos segura, que evita la pérdida de control de la información por el uso de múltiples archivos de texto que puedan contener información duplicada o errónea por falta de validaciones.

- Eficiencia. Con este sistema se disminuyen los tiempos de respuesta a requerimientos de otras áreas, debido a la automatización de muchos de los proceso, que con anterioridad tomaban un tiempo mucho mayor para su ejecución.

Como conclusión del estudio, es posible plantear que las aplicaciones de software y sistemas operativos sobre los que se hará el desarrollo y soportarán la aplicación, tienen la madurez y seguridad óptimas, y de acuerdo a las características de hardware con las que se cuenta se lograrán niveles de rendimiento y capacidades adecuados para la prestación de un buen servicio. Por lo anterior se considera factible la implantación del sistema de inventario de equipos, usuarios e incidentes de seguridad para formar parte de la operación del departamento de seguridad.

4.6 OBTENCIÓN DE REPORTES

El sistema de inventarios cuenta con un módulo de reportes en los cuales se refleja principalmente el estado de los inventarios en números y las actividades que se realizan sobre él, en intervalos de meses completos.

Los reportes deben ser obtenidos de forma comparativa, desde el primer mes del año en curso, es decir, enero, hasta el mes completo anterior terminado. Un ejemplo de ello, es la obtención de un reporte con la cantidad de equipos integrados al inventario sin importar la plataforma desde el mes de enero hasta el mes de julio, mostrando así la información de los meses enero, febrero, marzo, abril, mayo, junio, y julio. Finalmente se obtiene un promedio de la actividad mensual para un rubro específico.

El sistema genera un total de siete reportes, que contabilizan las actividades relacionadas con cada uno de los tres módulos del sistema: inventario de equipos, inventario de usuarios y seguimiento de incidentes de seguridad.

Todos los reportes son informativos para otras áreas de operación de la empresa, y podrán ser obtenidos por el personal de seguridad a través del sistema de inventarios, o bien, por el personal de otras áreas que tenga acceso al sitio de generación de reportes, y cuyo acceso es controlado por la aplicación de inventarios.

Todos los reportes se generan como un documento corporativo de la empresa en el cual se incluye un índice con el contenido del reporte, el objetivo, el desarrollo donde se da una descripción del documento, el detalle donde se presenta la tabla generada con los datos numéricos de la operación del sistema y las observaciones que pueden ser hechas en el momento en que éste se genera.

En la figura 4.6.1 se muestra el índice de uno de los reportes, y el cual es compartido por todos los demás.

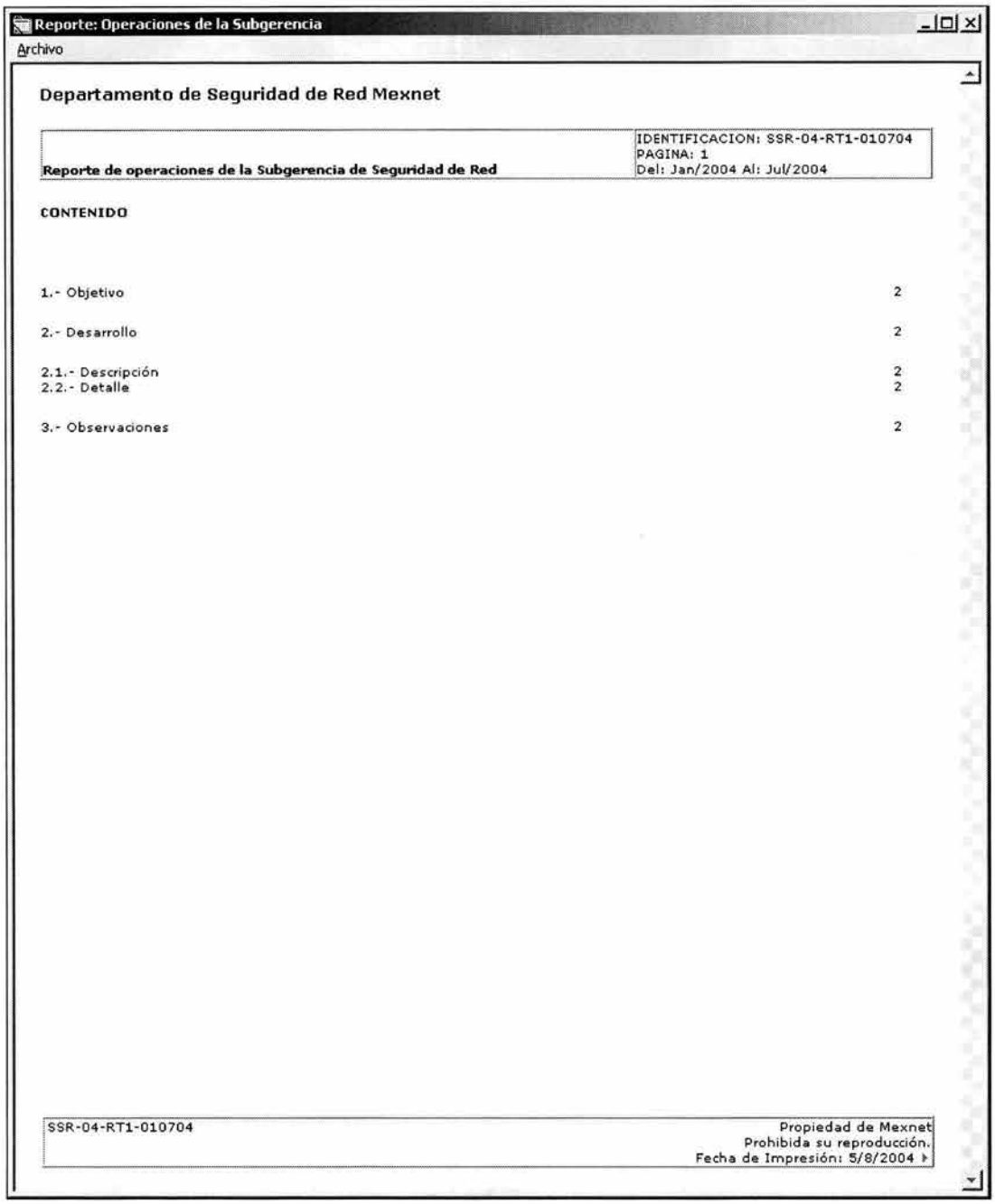
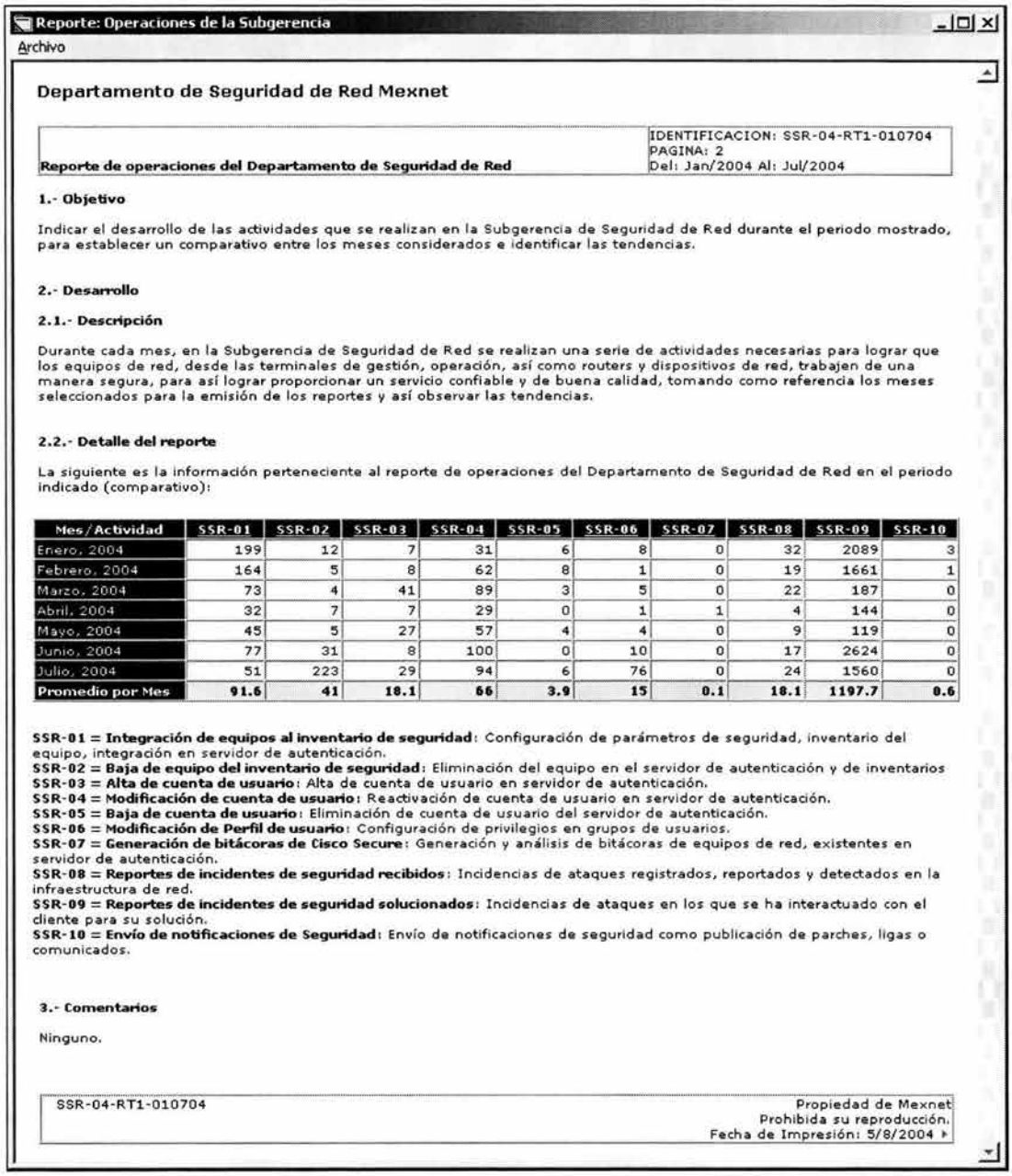


Figura 4.6.1 Indice del reporte.

En el índice se especifican los puntos que contiene el reporte.



Reporte: Operaciones de la Subgerencia

Archivo

Departamento de Seguridad de Red Mexnet

Reporte de operaciones del Departamento de Seguridad de Red	IDENTIFICACION: SSR-04-RT1-010704 PAGINA: 2 Del: Jan/2004 Al: Jul/2004

1.- Objetivo

Indicar el desarrollo de las actividades que se realizan en la Subgerencia de Seguridad de Red durante el periodo mostrado, para establecer un comparativo entre los meses considerados e identificar las tendencias.

2.- Desarrollo

2.1.- Descripción

Durante cada mes, en la Subgerencia de Seguridad de Red se realizan una serie de actividades necesarias para lograr que los equipos de red, desde las terminales de gestión, operación, así como routers y dispositivos de red, trabajen de una manera segura, para así lograr proporcionar un servicio confiable y de buena calidad, tomando como referencia los meses seleccionados para la emisión de los reportes y así observar las tendencias.

2.2.- Detalle del reporte

La siguiente es la información perteneciente al reporte de operaciones del Departamento de Seguridad de Red en el periodo indicado (comparativo):

Mes/Actividad	SSR-01	SSR-02	SSR-03	SSR-04	SSR-05	SSR-06	SSR-07	SSR-08	SSR-09	SSR-10
Enero, 2004	199	12	7	31	6	8	0	32	2089	3
Febrero, 2004	164	5	8	62	8	1	0	19	1661	1
Marzo, 2004	73	4	41	89	3	5	0	22	187	0
Abril, 2004	32	7	7	29	0	1	1	4	144	0
Mayo, 2004	45	5	27	57	4	4	0	9	119	0
Junio, 2004	77	31	8	100	0	10	0	17	2624	0
Julio, 2004	51	223	29	94	6	76	0	24	1560	0
Promedio por Mes	**91.6**	**41**	**18.1**	**66**	**3.9**	**15**	**0.1**	**18.1**	**1197.7**	**0.6**

SSR-01 = Integración de equipos al inventario de seguridad: Configuración de parámetros de seguridad, inventario del equipo, integración en servidor de autenticación.
SSR-02 = Baja de equipo del inventario de seguridad: Eliminación del equipo en el servidor de autenticación y de inventarios
SSR-03 = Alta de cuenta de usuario: Alta de cuenta de usuario en servidor de autenticación.
SSR-04 = Modificación de cuenta de usuario: Reactivación de cuenta de usuario en servidor de autenticación.
SSR-05 = Baja de cuenta de usuario: Eliminación de cuenta de usuario del servidor de autenticación.
SSR-06 = Modificación de Perfil de usuario: Configuración de privilegios en grupos de usuarios.
SSR-07 = Generación de bitácoras de Cisco Secure: Generación y análisis de bitácoras de equipos de red, existentes en servidor de autenticación.
SSR-08 = Reportes de incidentes de seguridad recibidos: Incidencias de ataques registrados, reportados y detectados en la infraestructura de red.
SSR-09 = Reportes de incidentes de seguridad solucionados: Incidencias de ataques en los que se ha interactuado con el cliente para su solución.
SSR-10 = Envío de notificaciones de Seguridad: Envío de notificaciones de seguridad como publicación de parches, ligas o comunicados.

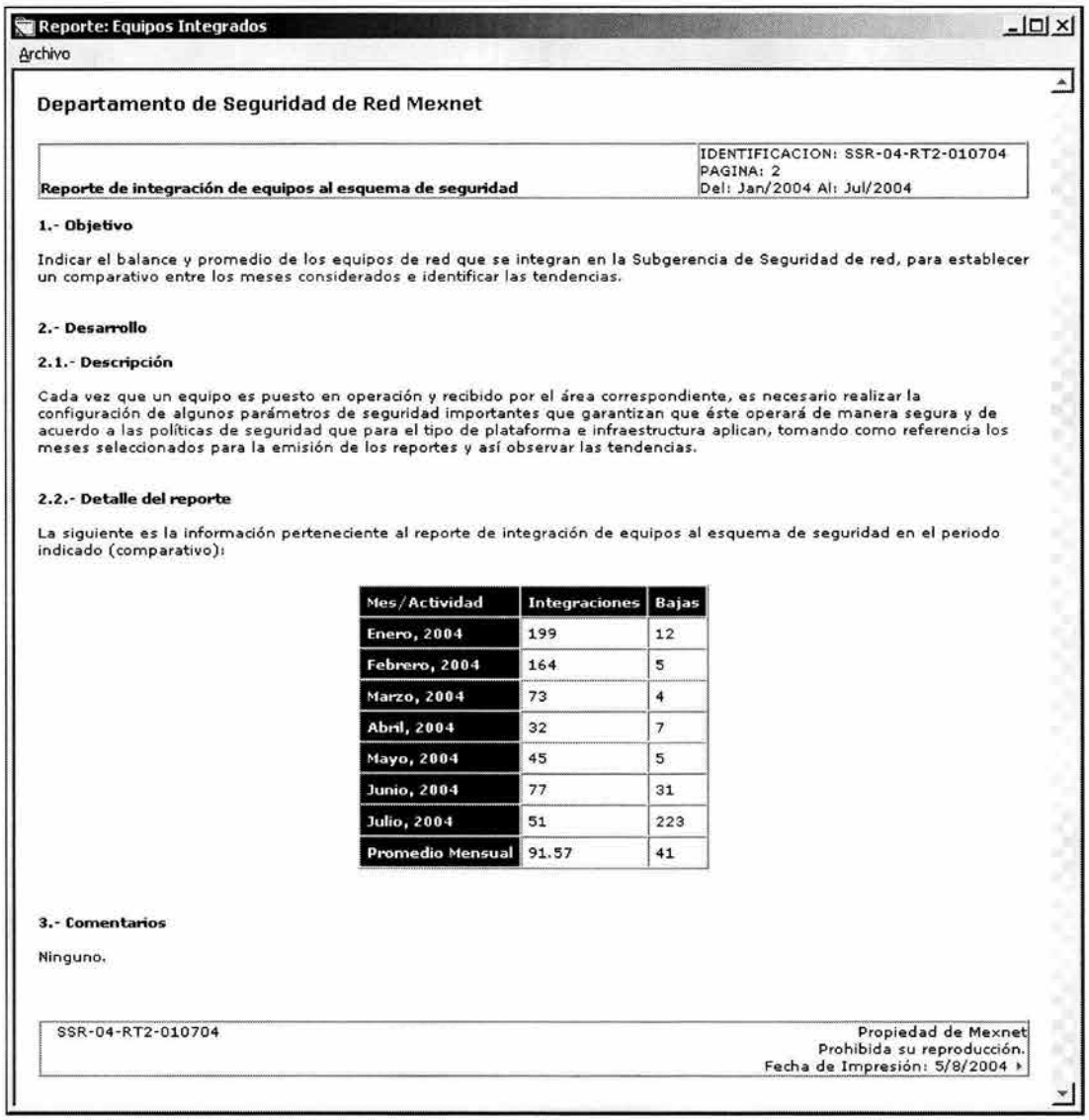
3.- Comentarios

Ninguno.

SSR-04-RT1-010704	Propiedad de Mexnet Prohibida su reproducción. Fecha de Impresión: 5/8/2004

Figura 4.6.2 Reporte de operaciones del departamento de seguridad.

Reporte de operaciones del departamento de seguridad (Figura 4.6.2). Su finalidad es contabilizar de manera general todas actividades realizadas por el área de seguridad y que son administradas por medio del sistema de inventarios.



Reporte: Equipos Integrados

Archivo

Departamento de Seguridad de Red Mexnet

Reporte de integración de equipos al esquema de seguridad	IDENTIFICACION: SSR-04-RT2-010704 PAGINA: 2 Del: Jan/2004 Al: Jul/2004

1.- Objetivo

Indicar el balance y promedio de los equipos de red que se integran en la Subgerencia de Seguridad de red, para establecer un comparativo entre los meses considerados e identificar las tendencias.

2.- Desarrollo

2.1.- Descripción

Cada vez que un equipo es puesto en operación y recibido por el área correspondiente, es necesario realizar la configuración de algunos parámetros de seguridad importantes que garantizan que éste operará de manera segura y de acuerdo a las políticas de seguridad que para el tipo de plataforma e infraestructura aplican, tomando como referencia los meses seleccionados para la emisión de los reportes y así observar las tendencias.

2.2.- Detalle del reporte

La siguiente es la información perteneciente al reporte de integración de equipos al esquema de seguridad en el periodo indicado (comparativo):

Mes/Actividad	Integraciones	Bajas
Enero, 2004	199	12
Febrero, 2004	164	5
Marzo, 2004	73	4
Abril, 2004	32	7
Mayo, 2004	45	5
Junio, 2004	77	31
Julio, 2004	51	223
Promedio Mensual	91.57	41

3.- Comentarios

Ninguno.

SSR-04-RT2-010704	Propiedad de Mexnet Prohibida su reproducción. Fecha de Impresión: 5/8/2004

Figura 4.6.3 Reporte de integración de equipos al inventario.

Cada vez que un equipo es puesto en operación y recibido por el área correspondiente, es necesario agregarlo al inventario de manera que sus datos puedan ser consultados en cualquier momento. El reporte de la figura 4.6.3 presenta la totalidad de equipos que fueron dados de alta en los inventarios sin importar la plataforma, solamente el conteo total en cada mes.

Reporte: Equipos Integrados por Plataforma

Archivo

Departamento de Seguridad de Red Mexnet

Reporte de equipos integrados al esquema de seguridad por plataforma	IDENTIFICACION: SSR-04-RT3-010704 PAGINA: 2 Del: Jan/2004 Al: Jul/2004

1.- Objetivo

Indicar el número de equipos de red integrados al esquema de seguridad de acuerdo a la plataforma y tipo, para establecer un comparativo entre los meses considerados e identificar las tendencias.

2.- Desarrollo

2.1.- Descripción

Cada vez que un equipo es puesto en operación y recibido por el área correspondiente, es necesario configurar algunos parámetros importantes que garantizan que éste operará de manera segura. Para cada tipo de plataforma que existe en la infraestructura de Uninet estos parámetros varían. Las plataformas que se manejan actualmente son Cisco, con sus modelos de routers: 2500, 3600, 7500, 12000, etc.; LAN Switches Catalyst, Network Access Servers 5300, 5800; equipos para ADSL, 7206; y Lucent con sus modelo Max TNT, Max 4000 y BSTDX Frame Relay Switches (FRSW), tomando como referencia los meses seleccionados para la emisión de los reportes y así observar las tendencias.

2.2.- Detalle del reporte

La siguiente es la información perteneciente al reporte de equipos integrados al esquema de seguridad por plataforma en el periodo indicado (comparativo):

Mes/Plataforma-Tipo	3640	7206	Catalyst	Hosts	INT	MaxTNT	Varios	VPDN	VPN
Enero, 2004	0	2	10	0	2	2	0	0	0
Febrero, 2004	0	0	3	0	8	2	0	0	1
Marzo, 2004	0	0	1	0	2	2	0	0	4
Abril, 2004	0	0	4	0	5	4	0	0	1
Mayo, 2004	0	4	4	0	9	1	0	0	4
Junio, 2004	1	2	8	0	9	1	0	0	10
Julio, 2004	0	1	2	0	5	4	0	0	3
Promedio Mensual	0.1	1.3	4.6	0	5.7	2.3	0	0	3.3

3640 = Cisco Routers 3640
7206 = Cisco Routers 7200
Catalyst = Cisco Catalyst
Hosts = Hosts y aplicaciones
INT = Cisco Routers Internet
MaxTNT = Lucent Max TNT
Varios = Cisco Varios
VPDN = Cisco Access Servers VPDN
VPN = Cisco Routers VPN

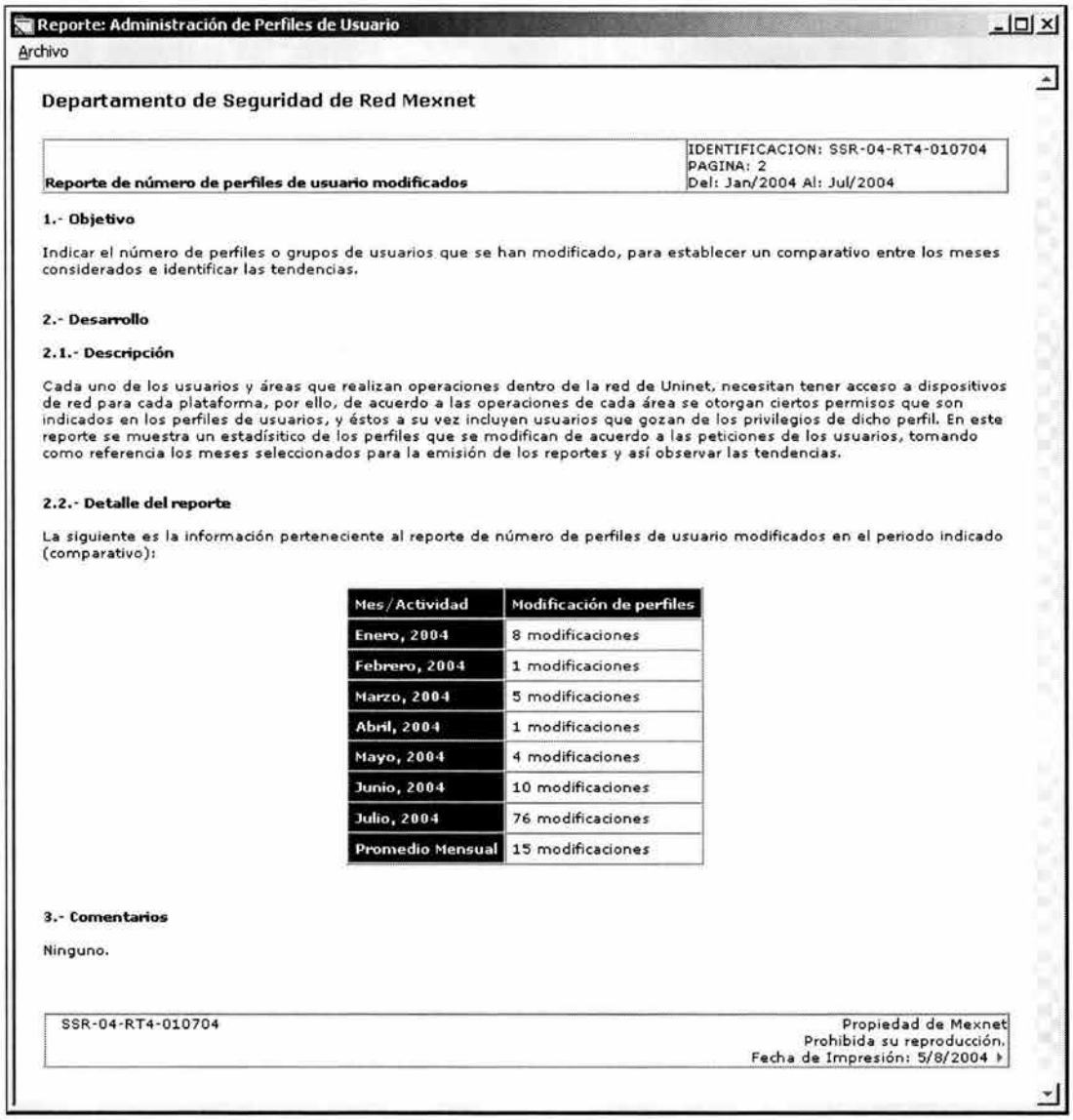
3.- Comentarios

Ninguno.

SSR-04-RT3-010704	Propiedad de Mexnet Prohibida su reproducción. Fecha de Impresión: 5/8/2004

Figura 4.6.4 Reporte de equipos integrados a los inventarios por plataforma

El reporte de la figura 4.6.4 presenta la totalidad de equipos que fueron dados de alta en los inventarios separados por plataforma.



Reporte: Administración de Perfiles de Usuario

Archivo

Departamento de Seguridad de Red Mexnet

Reporte de número de perfiles de usuario modificados	IDENTIFICACION: SSR-04-RT4-010704 PAGINA: 2 Del: Jan/2004 Al: Jul/2004

1.- Objetivo

Indicar el número de perfiles o grupos de usuarios que se han modificado, para establecer un comparativo entre los meses considerados e identificar las tendencias.

2.- Desarrollo

2.1.- Descripción

Cada uno de los usuarios y áreas que realizan operaciones dentro de la red de Uninet, necesitan tener acceso a dispositivos de red para cada plataforma, por ello, de acuerdo a las operaciones de cada área se otorgan ciertos permisos que son indicados en los perfiles de usuarios, y éstos a su vez incluyen usuarios que gozan de los privilegios de dicho perfil. En este reporte se muestra un estadísitico de los perfiles que se modifican de acuerdo a las peticiones de los usuarios, tomando como referencia los meses seleccionados para la emisión de los reportes y así observar las tendencias.

2.2.- Detalle del reporte

La siguiente es la información perteneciente al reporte de número de perfiles de usuario modificados en el periodo indicado (comparativo):

Mes / Actividad	Modificación de perfiles
Enero, 2004	8 modificaciones
Febrero, 2004	1 modificaciones
Marzo, 2004	5 modificaciones
Abril, 2004	1 modificaciones
Mayo, 2004	4 modificaciones
Junio, 2004	10 modificaciones
Julio, 2004	76 modificaciones
Promedio Mensual	15 modificaciones

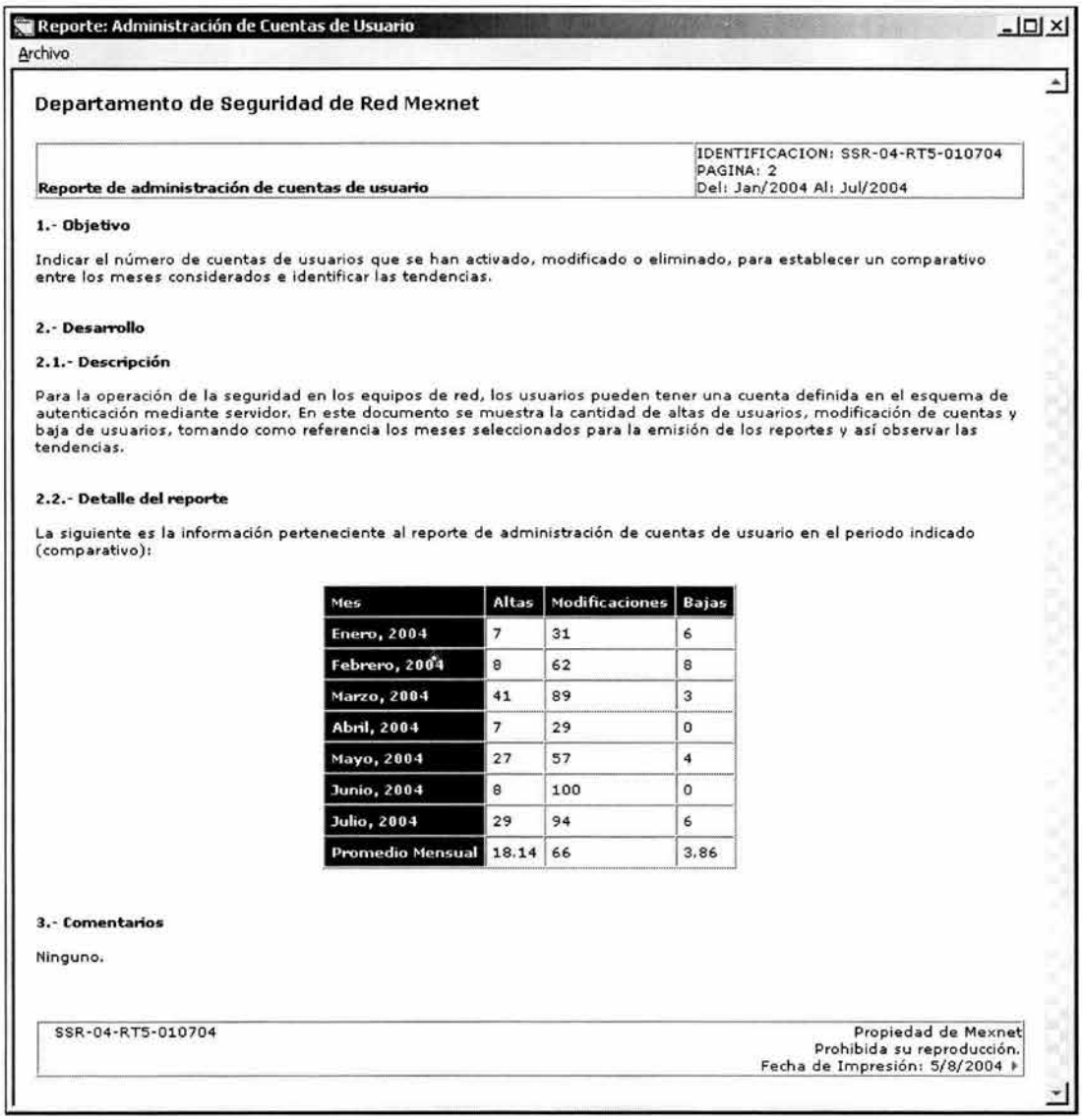
3.- Comentarios

Ninguno.

SSR-04-RT4-010704	Propiedad de Mexnet Prohibida su reproducción. Fecha de Impresión: 5/8/2004

Figura 4.6.5 Reporte de número de perfiles de usuario modificados

El reporte mostrado en la figura 4.6.5 presenta las operaciones de modificación que se realizaron durante los meses indicados a los perfiles de usuarios existentes en una categoría, mostrando únicamente la cantidad de movimientos existentes en cada mes. Estas modificaciones se refieren principalmente a cambios de privilegios en las plataformas de usuarios que soporte esta opción.



Reporte: Administración de Cuentas de Usuario

Archivo

Departamento de Seguridad de Red Mexnet

Reporte de administración de cuentas de usuario	IDENTIFICACION: SSR-04-RT5-010704 PAGINA: 2 Del: Jan/2004 Al: Jul/2004

1.- Objetivo

Indicar el número de cuentas de usuarios que se han activado, modificado o eliminado, para establecer un comparativo entre los meses considerados e identificar las tendencias.

2.- Desarrollo

2.1.- Descripción

Para la operación de la seguridad en los equipos de red, los usuarios pueden tener una cuenta definida en el esquema de autenticación mediante servidor. En este documento se muestra la cantidad de altas de usuarios, modificación de cuentas y baja de usuarios, tomando como referencia los meses seleccionados para la emisión de los reportes y así observar las tendencias.

2.2.- Detalle del reporte

La siguiente es la información perteneciente al reporte de administración de cuentas de usuario en el periodo indicado (comparativo):

Mes	Altas	Modificaciones	Bajas
Enero, 2004	7	31	6
Febrero, 2004	8	62	8
Marzo, 2004	41	89	3
Abril, 2004	7	29	0
Mayo, 2004	27	57	4
Junio, 2004	8	100	0
Julio, 2004	29	94	6
Promedio Mensual	18.14	66	3.86

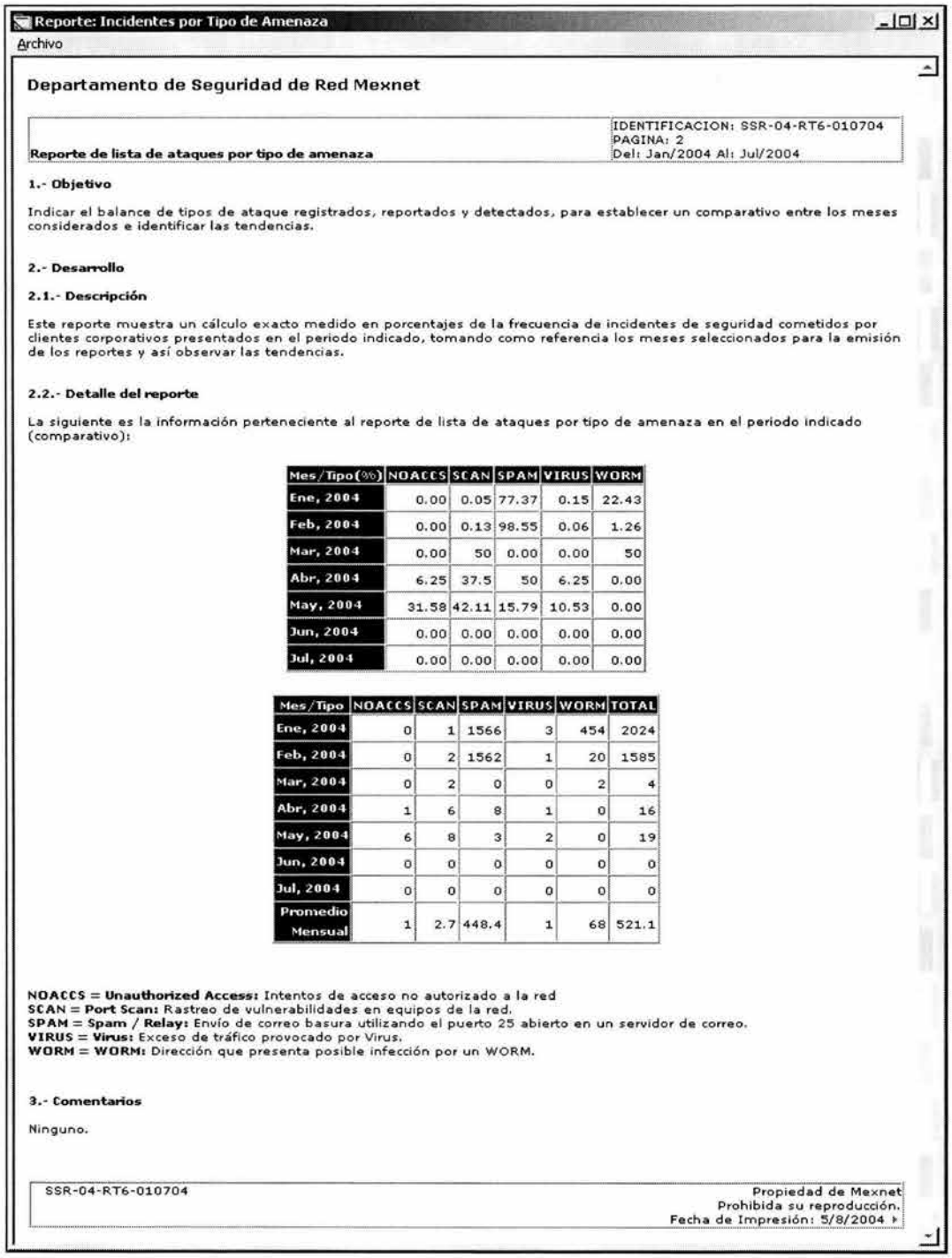
3.- Comentarios

Ninguno.

SSR-04-RT5-010704	Propiedad de Mexnet Prohibida su reproducción. Fecha de Impresión: 5/8/2004

Figura 4.6.6 Reporte de administración de cuentas de usuario

En el reporte de la figura 4.6.6, se proporciona un informativo de la cantidad de usuarios que se dan de alta, se modifican o se dan de baja en cada mes, presentando también su promedio. El número es presentado de manera global, incluyendo todos los usuarios sin importar su categoría.



Reporte: Incidentes por Tipo de Amenaza

Archivo

Departamento de Seguridad de Red Mexnet

Reporte de lista de ataques por tipo de amenaza	IDENTIFICACION: SSR-04-RT6-010704 PAGINA: 2 Del: Jan/2004 Al: Jul/2004

1.- Objetivo

Indicar el balance de tipos de ataque registrados, reportados y detectados, para establecer un comparativo entre los meses considerados e identificar las tendencias.

2.- Desarrollo

2.1.- Descripción

Este reporte muestra un cálculo exacto medido en porcentajes de la frecuencia de incidentes de seguridad cometidos por clientes corporativos presentados en el periodo indicado, tomando como referencia los meses seleccionados para la emisión de los reportes y así observar las tendencias.

2.2.- Detalle del reporte

La siguiente es la información perteneciente al reporte de lista de ataques por tipo de amenaza en el periodo indicado (comparativo):

Mes/Tipo(%)	NOACCS	SCAN	SPAM	VIRUS	WORM
Ene, 2004	0.00	0.05	77.37	0.15	22.43
Feb, 2004	0.00	0.13	98.55	0.06	1.26
Mar, 2004	0.00	50	0.00	0.00	50
Abr, 2004	6.25	37.5	50	6.25	0.00
May, 2004	31.58	42.11	15.79	10.53	0.00
Jun, 2004	0.00	0.00	0.00	0.00	0.00
Jul, 2004	0.00	0.00	0.00	0.00	0.00

Mes/Tipo	NOACCS	SCAN	SPAM	VIRUS	WORM	TOTAL
Ene, 2004	0	1	1566	3	454	2024
Feb, 2004	0	2	1562	1	20	1585
Mar, 2004	0	2	0	0	2	4
Abr, 2004	1	6	8	1	0	16
May, 2004	6	8	3	2	0	19
Jun, 2004	0	0	0	0	0	0
Jul, 2004	0	0	0	0	0	0
Promedio Mensual	1	2.7	448.4	1	68	521.1

NOACCS = Unauthorized Access: Intentos de acceso no autorizado a la red
SCAN = Port Scan: Rastreo de vulnerabilidades en equipos de la red.
SPAM = Spam / Relay: Envío de correo basura utilizando el puerto 25 abierto en un servidor de correo.
VIRUS = Virus: Exceso de tráfico provocado por Virus.
WORM = WORM: Dirección que presenta posible infección por un WORM.

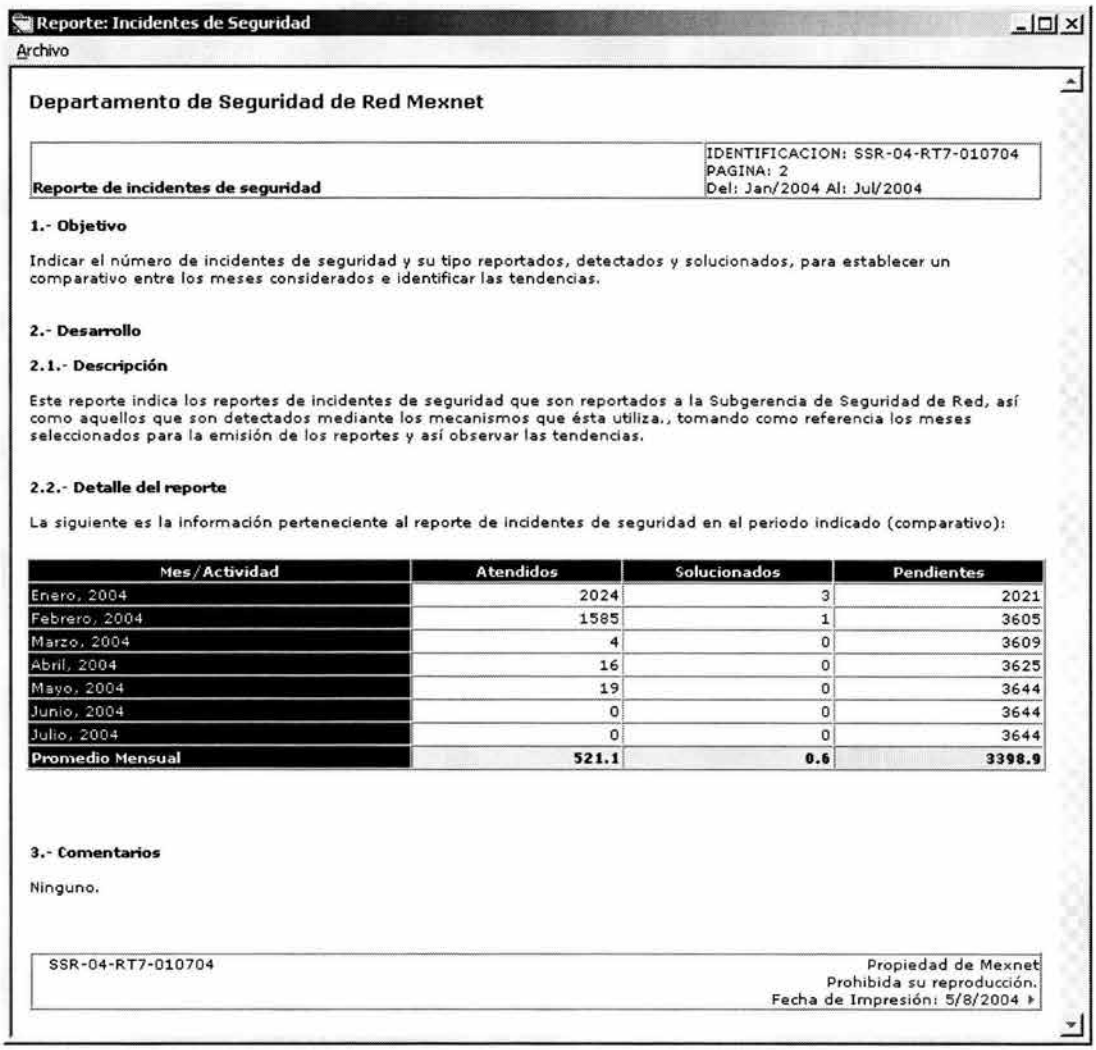
3.- Comentarios

Ninguno.

SSR-04-RT6-010704	Propiedad de Mexnet Prohibida su reproducción. Fecha de Impresión: 5/8/2004

Figura 4.6.7 Reporte de incidentes de seguridad por tipo de amenaza

En el reporte de la figura 4.6.7, se muestra la totalidad de los incidentes de seguridad reportados al área y separados por tipo de incidente.



Reporte: Incidentes de Seguridad

Archivo

Departamento de Seguridad de Red Mexnet

Reporte de incidentes de seguridad	IDENTIFICACION: SSR-04-RT7-010704 PAGINA: 2 Del: Jan/2004 Al: Jul/2004

1.- Objetivo

Indicar el número de incidentes de seguridad y su tipo reportados, detectados y solucionados, para establecer un comparativo entre los meses considerados e identificar las tendencias.

2.- Desarrollo

2.1.- Descripción

Este reporte indica los reportes de incidentes de seguridad que son reportados a la Subgerencia de Seguridad de Red, así como aquellos que son detectados mediante los mecanismos que ésta utiliza., tomando como referencia los meses seleccionados para la emisión de los reportes y así observar las tendencias.

2.2.- Detalle del reporte

La siguiente es la información perteneciente al reporte de incidentes de seguridad en el periodo indicado (comparativo):

Mes/Actividad	Atendidos	Solucionados	Pendientes
Enero, 2004	2024	3	2021
Febrero, 2004	1585	1	3605
Marzo, 2004	4	0	3609
Abril, 2004	16	0	3625
Mayo, 2004	19	0	3644
Junio, 2004	0	0	3644
Julio, 2004	0	0	3644
Promedio Mensual	**521.1**	**0.6**	**3398.9**

3.- Comentarios

Ninguno.

SSR-04-RT7-010704	Propiedad de Mexnet Prohibida su reproducción. Fecha de Impresión: 5/8/2004

Figura 4.6.8 Reporte de incidentes de seguridad

El reporte de la figura 4.6.8 presenta el total de incidentes que son atendidos por el área de seguridad, sin importar el tipo de amenaza, pero indicando que cantidad del total de incidentes atendidos son resueltos y cerrados por el departamento de seguridad, y cuantos quedan pendientes por resolver.

MANUAL DE USUARIO

1.1 Descripción general

El sistema de administración de inventarios de equipos y usuarios e incidentes de seguridad permite organizar la información de inventarios de equipos y usuarios que acceden a los servicios de red mediante la generación de grupos de trabajo, así como el seguimiento a los reportes de incidentes de seguridad.

Cuenta con la información actualizada del catálogo de equipos de red que se encuentran en operación, los usuarios que tienen acceso a ellos, y permite el envío de mensajes automáticos.

Con la base de datos centralizada se lleva el control de las cuentas de acceso asignadas a los usuarios, la clasificación de los equipos de red de acuerdo a su función y la información de los reportes e incidentes de seguridad que se reciben.

El sistema opera bajo un esquema cliente servidor para dar un ambiente de alta velocidad al manejo y envío de los reportes lo que permite reducir los tiempos de operación del departamento de seguridad de red y minimizar la posibilidad de errores en el proceso de la información.

El sistema es operado por el personal del área de seguridad de la empresa.

1.2 Acceso al sistema

Para iniciar una sesión en el sistema, figura 1.2.1, se solicita el nombre del usuario que es Administrador y la contraseña, la cual es configurada en cada una de las terminales donde el sistema es instalado.

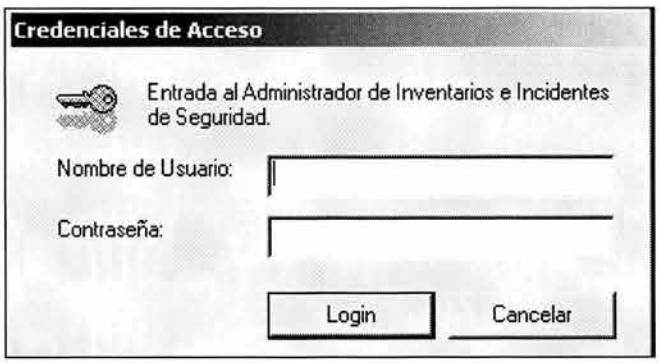


Figura 1.2.1 Validación de entrada al sistema.

Si se introduce una información de acceso no válida, se despliega una ventana que notifica que la información de acceso es incorrecta, figura 1.2.2.

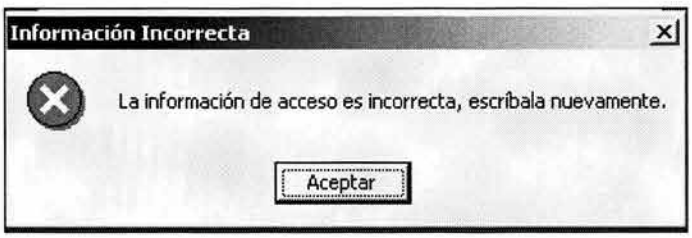


Figura 1.2.2 Información no válida de acceso.

Al validar una cuenta existente, se despliega la pantalla inicial del sistema, en la que se muestran el menú principal, la barra de herramientas, la barra de estado, figura 1.2.3.

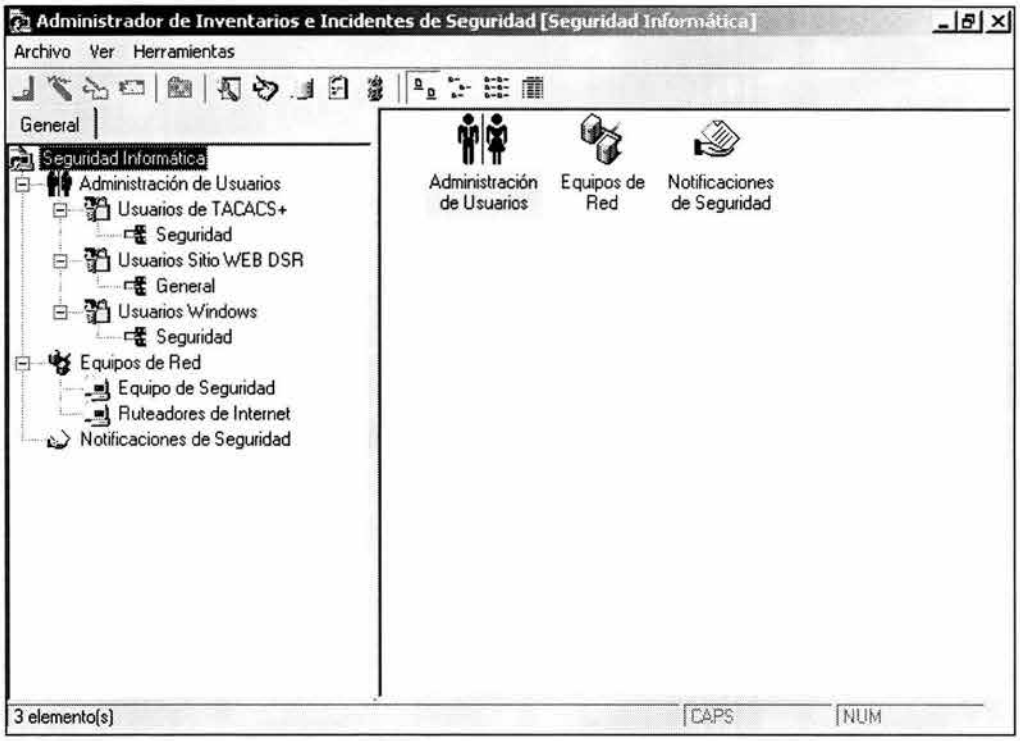


Figura 1.2.3 Ventana principal del sistema.

El sistema cuenta con tres módulos principales:

- Administración de usuarios
- Equipos de red y
- Notificaciones de seguridad

1.3 Administración de usuarios

El módulo de administración de usuarios, permite crear el grupo de trabajo en el que se agruparán los usuarios para su control. Por default, se tienen tres grupos de trabajo:

- Usuarios de TACACS+
- Usuarios de desarrollo de sitios WEB y
- Usuarios de Windows

Para la creación de una nueva categoría de usuarios, se selecciona administración de usuarios del árbol, se da clic en la opción *Archivo* del menú principal y se despliega la ventana de la figura 1.3.1.

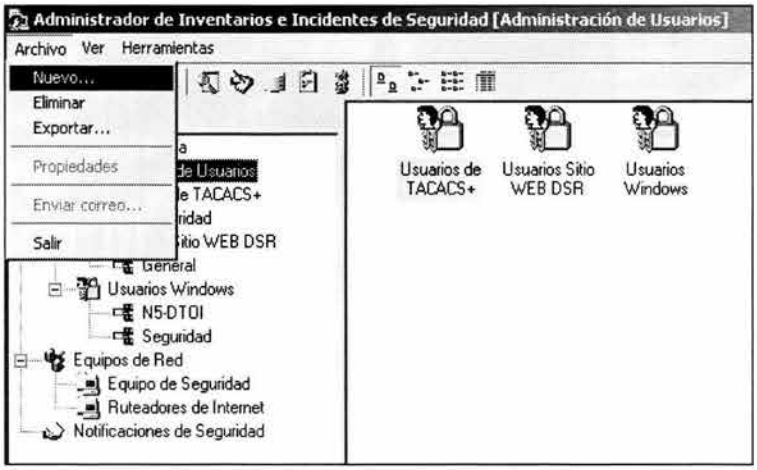


Figura 1.3.1 Creación de categorías de usuarios.

Se da clic en *Nuevo* del menú *Archivo* y se abre la pantalla Nueva Categoría de Usuarios, como se muestra en la figura 1.3.2.

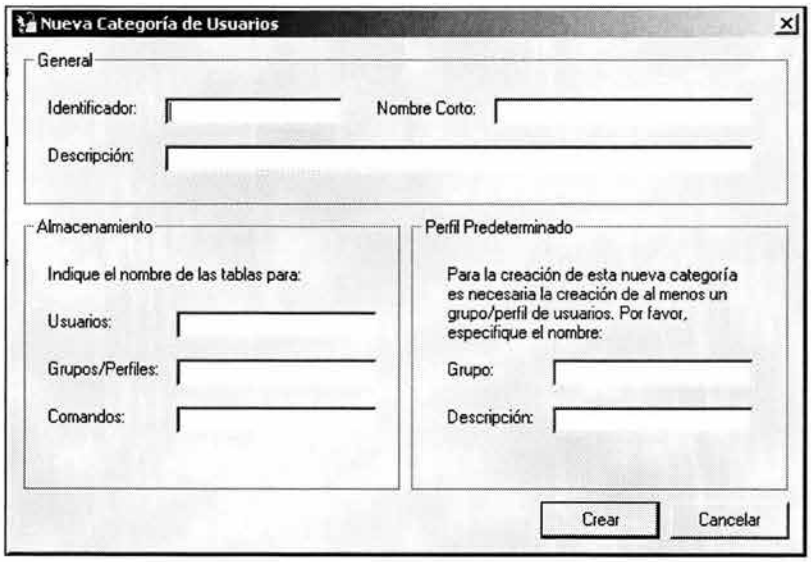


Figura 1.3.2 Parámetros para una nueva categoría de usuarios.

Se llenan los campos solicitados en la pantalla. En la sección de Almacenamiento se generan automáticamente los nombres de las tablas donde será almacenada la información, de acuerdo al identificador especificado en el campo correspondiente. Al terminar de capturar la información, se da clic en el botón *Crear* para dar de alta el grupo o se da clic en el botón *Cancelar* para cancelar la creación del grupo. En el primer caso, se despliega el mensaje de la figura 1.3.3 que informa que la nueva categoría de usuarios de creó con éxito.

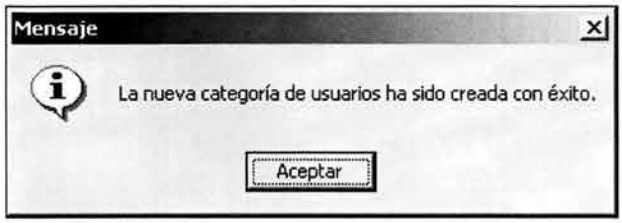


Figura 1.3.3 Creación exitosa de una categoría.

Se crea un icono en la pantalla principal del sistema que incluye ahora la nueva categoría y su grupo (Usuarios Nuevos). Figura 1.3.4.

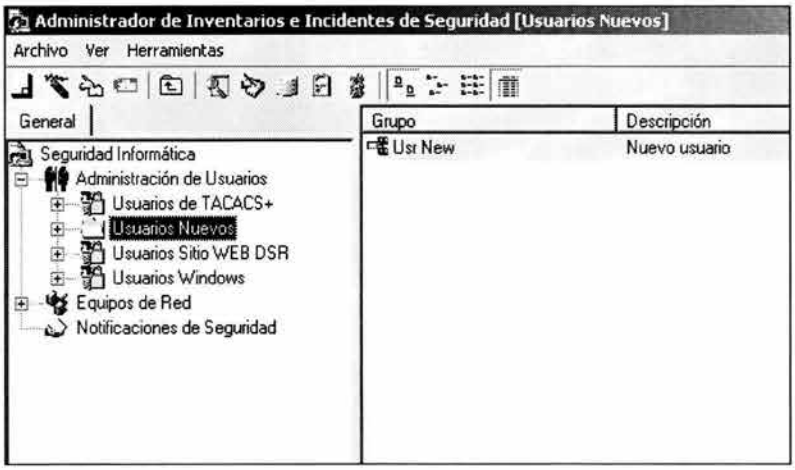


Figura 1.3.4 Nueva categoría creada.

Para crear un perfil en la categoría creada, se selecciona la opción *Nuevo* del menú principal y se despliega la pantalla de la figura 1.3.5.

Figura 1.3.5 Creación de un nuevo perfil o grupo.

Se captura el nombre y la descripción del nuevo grupo y se presiona el botón *Aceptar* para crearlo o el botón *Cancelar* para cancelar la petición. Al aceptar se crea el nuevo grupo y se podrán agregar a él los usuarios que pertenecen a éste, figura 1.3.6.

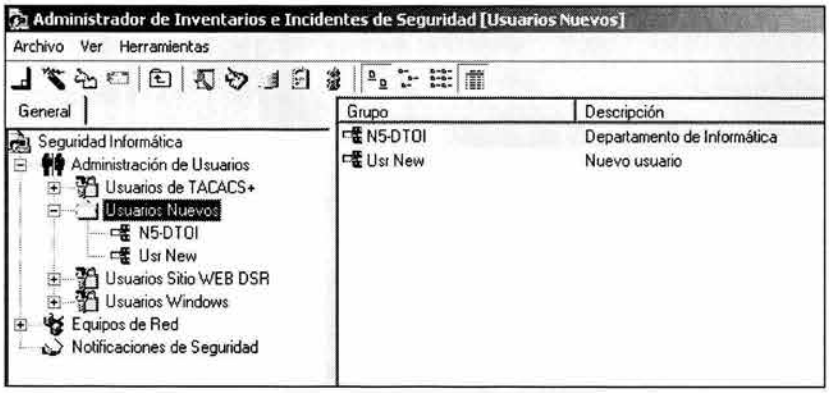


Figura 1.3.6 Creación terminada del nuevo perfil o grupo.

Se posiciona el cursor en el nuevo grupo (Usuarios Nuevos) y del menú principal, se selecciona la opción *Nuevo* apareciendo la pantalla de la figura 1.3.7; para crear un nuevo usuario se captura la información solicitada y se presiona el botón *Aplicar* para crear el usuario, así sucesivamente hasta terminar la creación de éstos. Los botones *Gen* generarán las contraseñas de los usuarios de forma aleatoria de acuerdo a las políticas establecidas por la empresa y el área de seguridad.

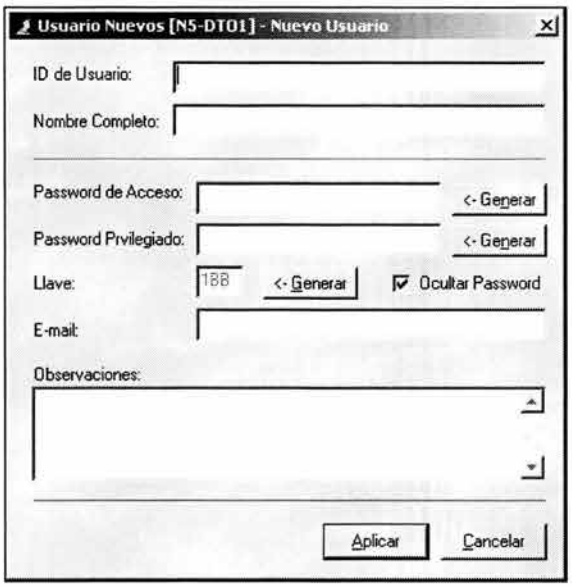


Figura 1.3.7 Creación de un nuevo usuario.

Una vez concluido el proceso de alta de los usuarios, éstos se identifican en la pantalla inicial del sistema por medio de iconos con el nombre del usuario.

1.4 Administración de equipos de red

Este módulo por default viene configurado con las opciones para administrar Equipos de seguridad y Ruteadores de Internet, como se muestra en la figura 1.4.1.

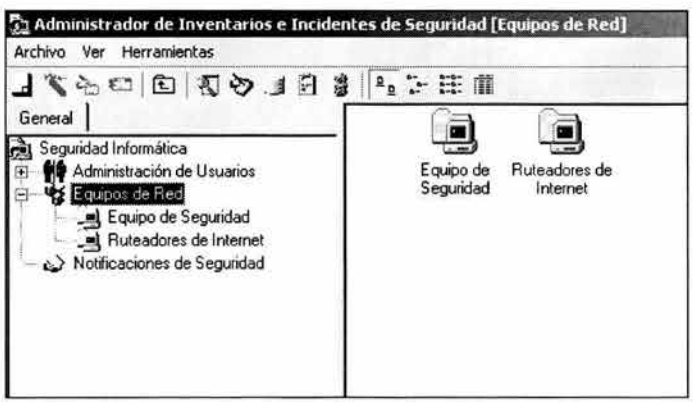


Figura 1.4.1 Administración de equipos de red.

Para crear una nueva plataforma de equipos, en el menú principal dar clic en *Archivo* y seleccionar *Nuevo*; se despliega la pantalla de la figura 1.4.2 en la que se captura la información solicitada.

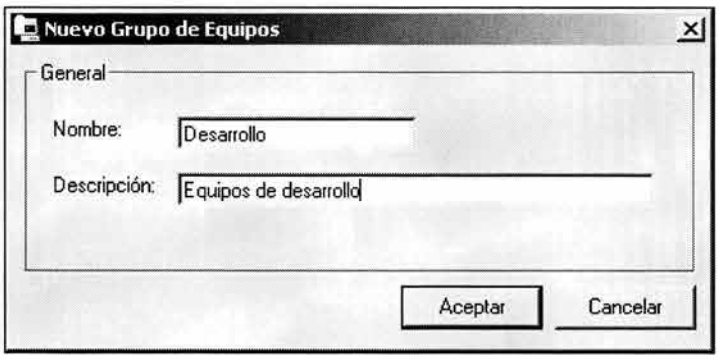


Figura 1.4.2 Creación de un nuevo grupo o plataforma de equipos.

Se da clic en el botón *Aceptar* para crear el grupo o se da clic en *Cancelar* para no realizar la acción. Para dar de alta en alguno de los grupos existentes se selecciona del menú principal la opción *Archivo* y se da clic en *Nuevo*, desplegándose la pantalla de la figura 1.4.3.

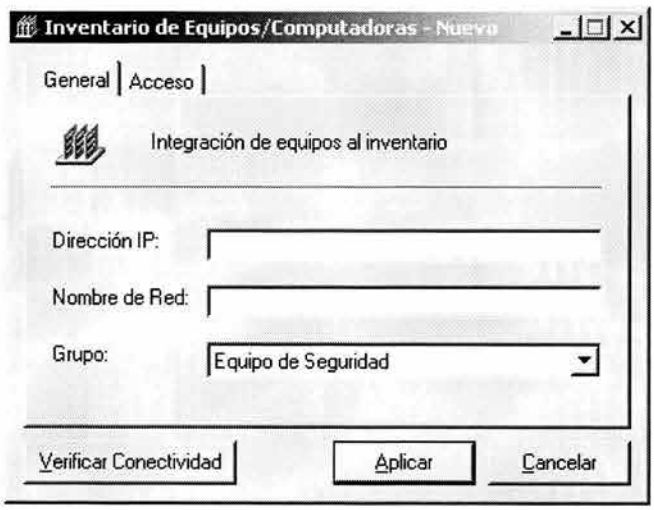


Figura 1.4.3 Alta de un nuevo equipo al inventario.

Se especifica la dirección IP, el nombre de equipo de red y se selecciona el grupo al que pertenecerá para su administración. Para verificar la conectividad de la IP asignada se da clic en el botón *Verificar Conectividad* y el sistema genera un ping a la misma en modo MS-DOS. En caso de que la verificación sea correcta se da clic en el botón *Aplicar*. En el tabulador *Acceso* se generan las contraseñas de Telnet o de Enable/Admin, figura 1.4.4, para los equipos que requieran configuración local de contraseñas. Si se presiona el botón *Gen* correspondiente, la contraseña será generada aleatoriamente de acuerdo a las políticas establecidas por la empresa.

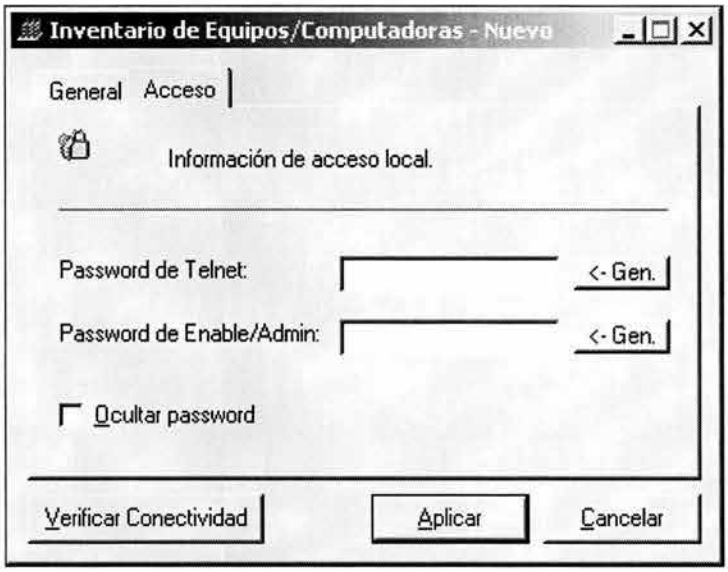


Figura 1.4.4 Generación y captura de contraseñas.

1.5 Notificaciones de seguridad

El módulo de Notificaciones de Seguridad se utiliza para enviar avisos que pueden ser desde ataques de virus, hasta de información interna, por dos medios; de forma masiva (seleccionando el grupo de trabajo) y por usuario, especificando la cuenta de correo electrónico (uno o más destinatarios).

Estando seleccionado el módulo Notificaciones de Seguridad en la pantalla inicial del sistema, se habilita el botón *Archivo* y se selecciona la opción *Nuevo*, desplegándose la pantalla de la figura 1.5.1.

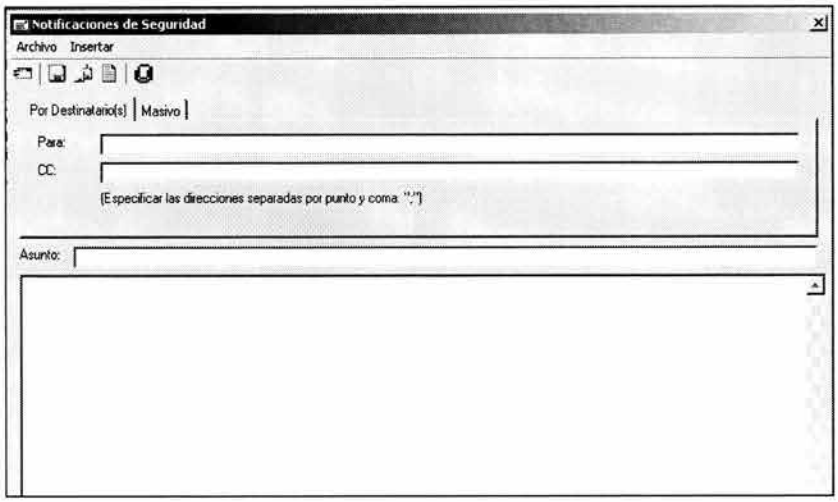


Figura 1.5.1 Notificaciones de Seguridad.

El menú *Insertar* de este módulo, *Archivo* para incluir un archivo adjunto y *Firma DSR* para la firma del Departamento de Seguridad de Red como se muestra en las figuras 1.5.2 y 1.5.3.

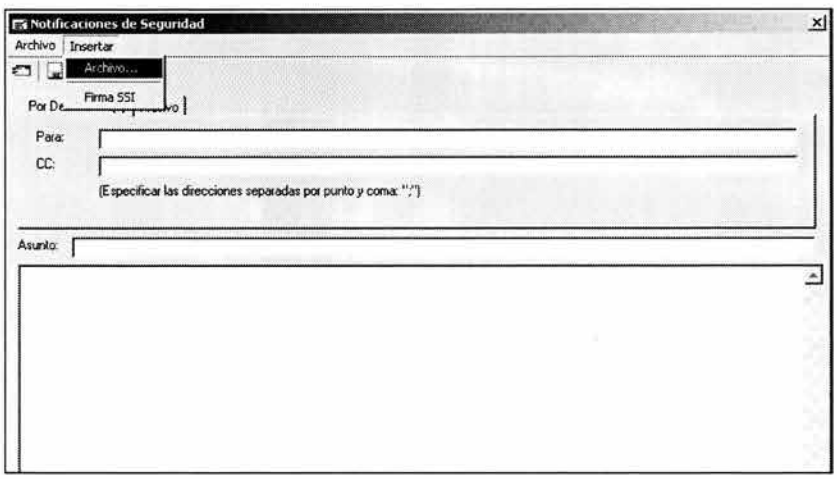


Figura 1.5.2 Menú Insertar.

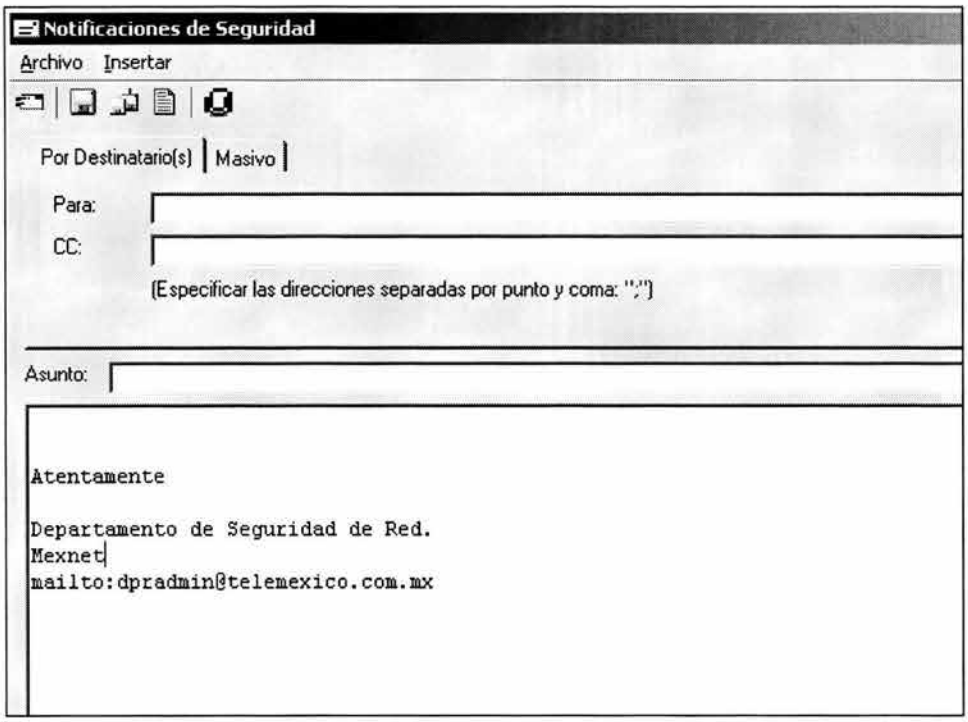


Figura 1.5.3 Insertar Firma DSR.

El menú tiene también el botón *Archivo* con las opciones *Enviar, Guardar, Guardar Como, Guardar como Archivo y Salir*, figura 1.5.4. Una vez que se llenan los campos solicitados, la notificación se envía activando el botón *Archivo* y seleccionando la opción *Enviar*, o bien mediante el botón Enviar de la barra de herramientas.

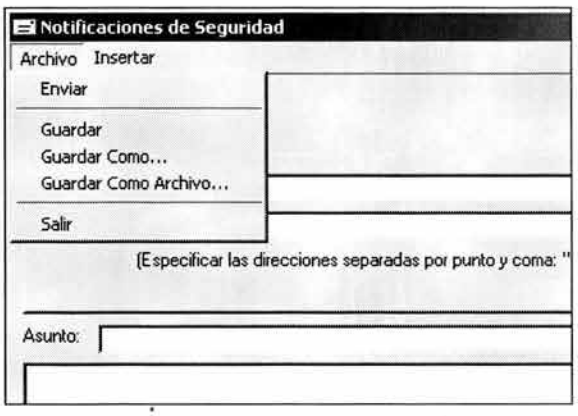


Figura 1.5.4 Menú Archivo de la ventana de notificaciones de seguridad.

Al enviar la notificación, el sistema informa que esta ha sido enviada con éxito.
Es posible guardar en la base de datos las notificaciones creadas, con el fin de que en caso de enviarse nuevamente no sea necesaria la captura nuevamente. Para guardar la notificación se selecciona la opción del menú *Archivo* o se presiona sobre el botón correspondiente de la barra de herramientas.

1.6 Funciones del menú principal

La pantalla inicial del sistema cuenta con un menú principal, que integra opciones de navegación rápida en el mismo, siendo las principales las siguientes:

- Archivo
- Ver
- Herramientas

Las opciones de cada una se muestran en las figuras 1.6.1, 1.6.2 y 1.6.3 siguientes:

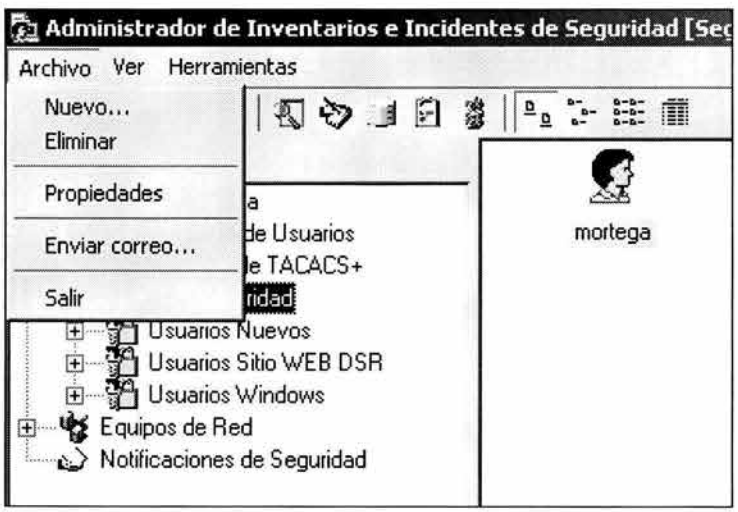


Figura 1.6.1 Menú Archivo de la ventana principal del sistema.

En este submenú, dependiendo el módulo activo, se da de alta un nuevo registro en el sistema (usuario, grupo o notificación) con la opción *Nuevo...*; se da de baja un registro existente con la opción *Eliminar*; se muestran las propiedades del registro existente con la opción *Propiedades*; se habilita el módulo Enviar Notificaciones con la opción *Enviar correo...* ó se concluye la sesión en el sistema con la opción *Salir*.

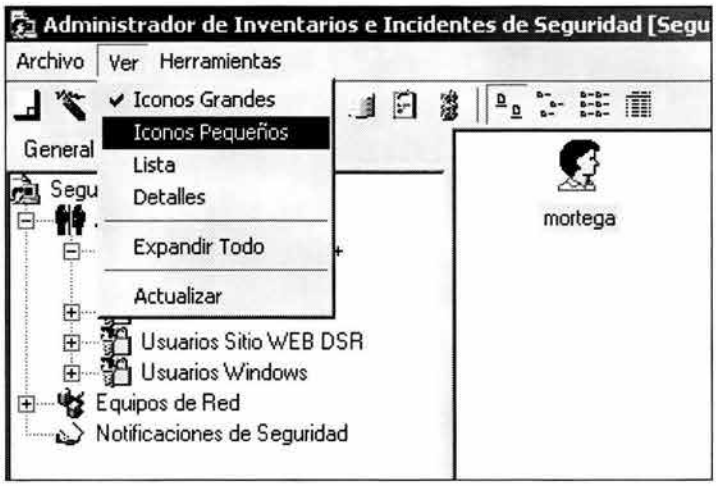


Figura 1.6.2 Menú Ver.

Este submenú, permite visualizar el aspecto de los íconos y también tiene la opción de expandir automáticamente todos los registros de cada módulo y permite actualizar los datos mostrados realizando una consulta a la base de datos, con la opción Actualizar.

En la figura 1.6.3 se muestra el menú *Herramientas,* mediante el cual se realizan las actividades relacionadas con la administración y seguimiento de incidentes de seguridad que incluye la consulta de existentes y la captura de nuevos. Asimismo es posible el envío de las notificaciones automáticas derivadas de la captura de estos incidentes, mediante el menú *Notificación de Incidentes*.

En la opción *Bitácoras* es posible obtener las bitácoras de administración de los equipos de red, que se obtiene del servidor de Cisco Secure y la bitácora de acceso al sitio WEB para obtención de reportes.

La opción *Reportes de Actividades* permite la obtención de los reportes de operación del sistema. La opción de *Notificación Masiva de Contraseñas*, permite el envío automático de todas las cuentas de usuario existentes en una categoría.

La opción de *Búsquedas* permite realizar consultas de equipos, usuarios e incidentes registrados en la base de datos, indicando la fecha en la que se realizó la actividad, y las características principales del registro.

La opción *Encriptador/Desencriptador* es una herramienta útil para obtener la encriptación de, por ejemplo, una contraseña de manera informativa.

En *Opciones* es posible la especificación de los parámetros de operación del sistema, como la contraseña de acceso al mismo, la longitud de las contraseñas que se generan en los módulos de equipos y usuarios, o las rutas de acceso para el procesamiento de las bitácoras de Cisco Secure.

En la figura 1.6.3 se muestran las opciones del menú *Herramientas* de la ventana principal del sistema.

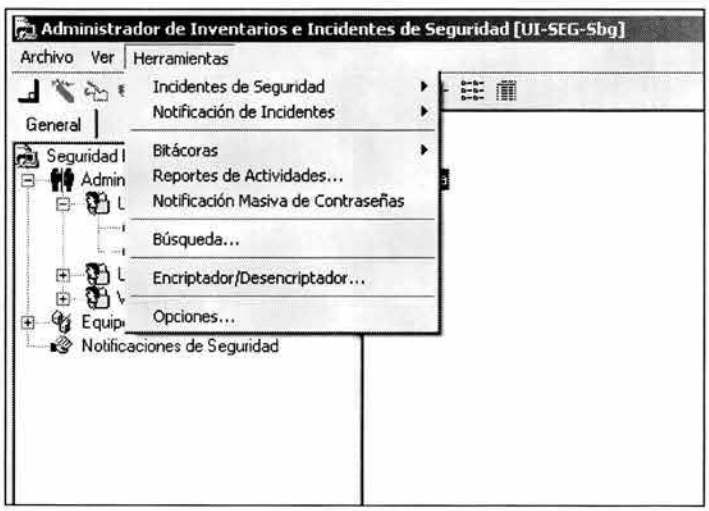


Figura 1.6.3 Menú Herramientas

1.7 Incidentes de seguridad

Para la captura de un incidente de seguridad, se selecciona la opción *Edición de Incidentes* de la opción *Incidentes de Seguridad* del menú de herramientas, obteniendo la ventana de captura como la mostrada en la figura 1.7.1.

Figura 1.7.1 Edición de incidentes de seguridad.

Es necesaria la captura de todos los campos para dar de alta un incidente de seguridad, tanto de la pestaña *Incidente*, como de la pantalla *Contacto* en la cual se especifica la información necesaria para el envío de la notificación de incidente automática. En la figura 1.7.2 se muestra la pestaña *Contacto*.

Al terminar la captura del incidente es necesario presionar el botón *Registrar* para almacenar el reporte en la base de datos.

Una vez capturado el o los incidentes se envían las notificaciones correspondientes mediante la opción *Notificación de Incidentes*.

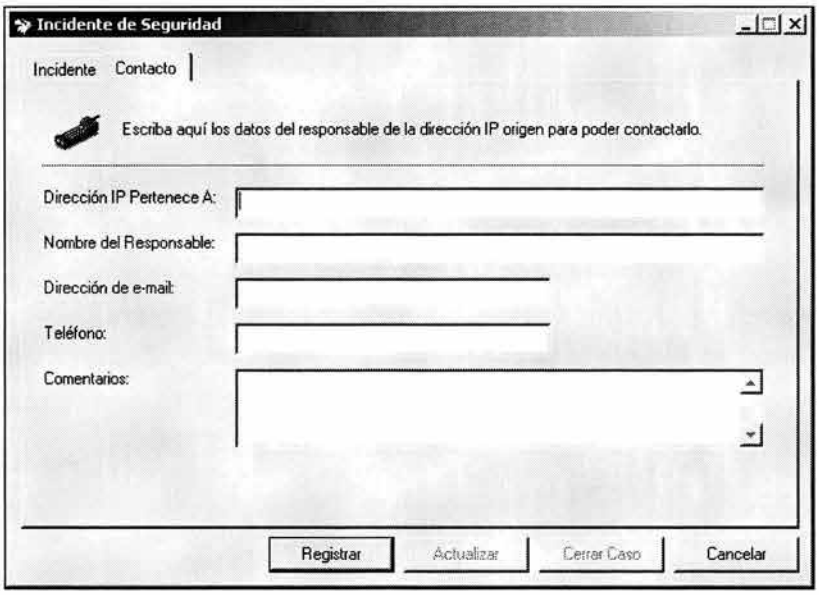


Figura 1.7.2 Edición de incidentes de seguridad.

1.8 Bitácoras

Para obtener las bitácoras de Cisco Secure, se selecciona la opción *Bitácoras, Cisco Secure Logs*. En la figura 1.8.1 se muestra la ventana donde se especifican los parámetros de búsqueda.

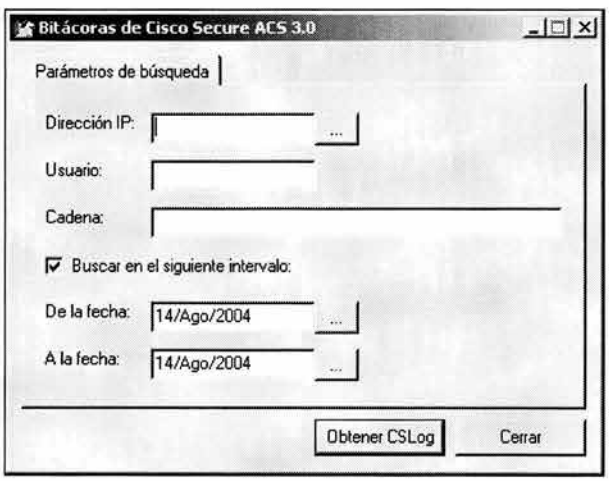


Figura 1.8.1 Bitácoras de Cisco Secure.

1.9 Búsquedas

Al seleccionar la opción de *Búsqueda* es posible realizar una consulta de incidentes, equipos y usuarios. Las figuras 1.9.1, 1.9.2 y 1.9.3, se muestran las opciones.

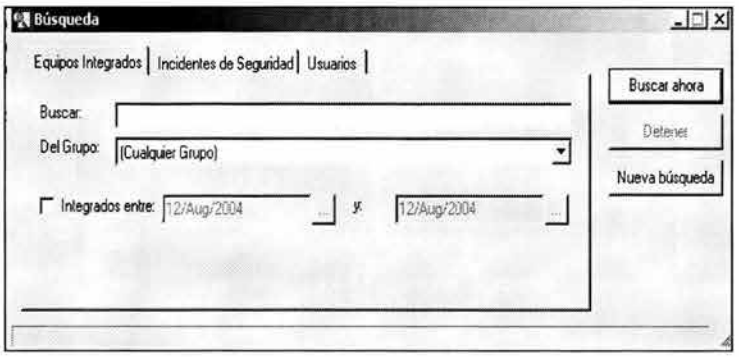


Figura 1.9.1 Consulta de equipos integrados.

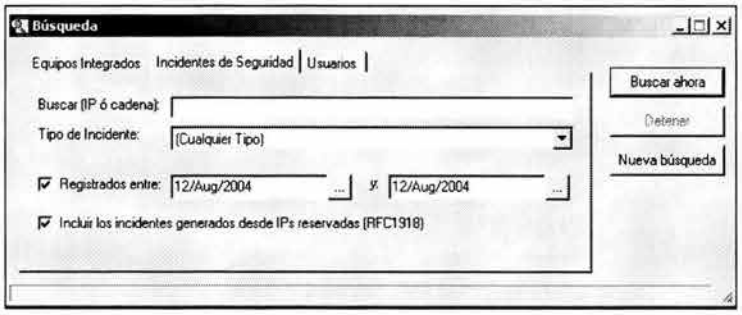


Figura 1.9.2 Consulta de Incidentes.

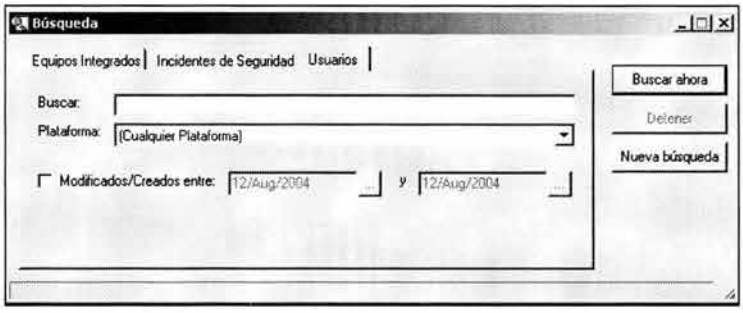


Figura 1.9.3 Consulta de usuarios registrados.

1.10 Reportes

Al especificar los parámetros de búsqueda y presionar el botón *Buscar ahora* se muestran los resultados en la parte inferior de la ventana.

Para la obtención de reportes, se selecciona la opción *Reportes de actividades*, mostrado el cuadro de diálogo de la figura 1.10.1. Se especifican los parámetros de tipo de reporte, meses y año, y se presiona Aceptar para obtenerlos. Si se desea , se pueden agregar comentarios al reporte.

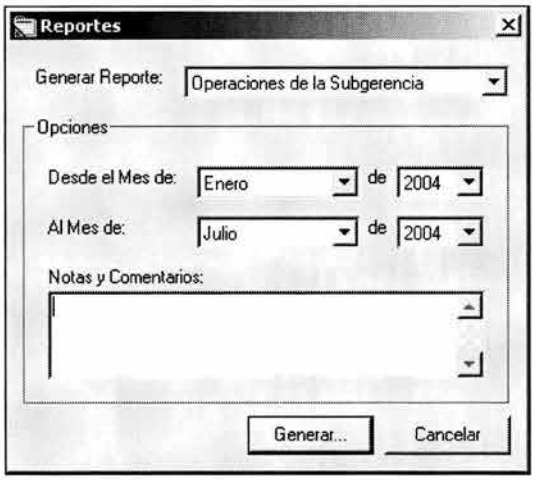


Figura 1.10.1 Obtención de reportes.

1.11 Opciones

En ventana de la figura 1.11.1, se especifican las opciones de operación del sistema. En ella se especifica la longitud de las contraseñas que genera el sistema, la ruta donde se almacenan las bitácoras y la contraseña de acceso al sistema en la terminal donde se encuentra instalado.

Función 1.11.1 Opciones del sistema.

MANUAL TÉCNICO

2.1 Descripción general

En el presente manual se presentan algunos procedimientos importantes a considerar para la operación óptima del sistema y su base de datos, así como para mantener la seguridad de la información y que, para casos emergentes se tenga la disponibilidad de ella, de una manera rápida y segura.

Existen dos procedimientos básicos a describir, los cuales son aplicables directamente a la base de datos de SQL, y que se enfocan a mantener copias de la información en medios de almacenamiento adicionales al servidor de producción, los cuales pueden irse actualizando a lo largo de la operación del sistema.

Estos procedimientos son:

- El respaldo de la base de datos.
- La restauración de un respaldo de la base de datos.

El respaldo de la base de datos es necesario a fin de tener la información del sistema en un sitio independiente al servidor de base de datos, para que, en casos de una eventualidad, ésta pueda ser obtenida rápidamente y restituida para su puesta en operación nuevamente.

La restauración es el proceso inverso al respaldo de la base de datos, y consiste en escribir nuevamente los datos guardados en el archivo de respaldo a las tablas de la base de datos del servidor de producción. Este proceso no se ejecuta de forma frecuente, solo en ocasiones especiales en las que se pierde información del servidor por fallas, o bien, si se desea cambiar el equipo que guarda la base de datos. Sin embargo, es importante este proceso, para aplicarlo en estas situaciones especiales.

2.2 Respaldo de la base de datos

Para realizar un respaldo se utiliza el SQL Enterprise Manager. Una vez que se selecciona la base de datos 'ssrdbsql' se deberá presionar sobre la opción *Backup Database* dentro de la opción *Todas las tareas*, del menú contextual de nuestra base de datos, como se muestra en la figura 2.1.1.

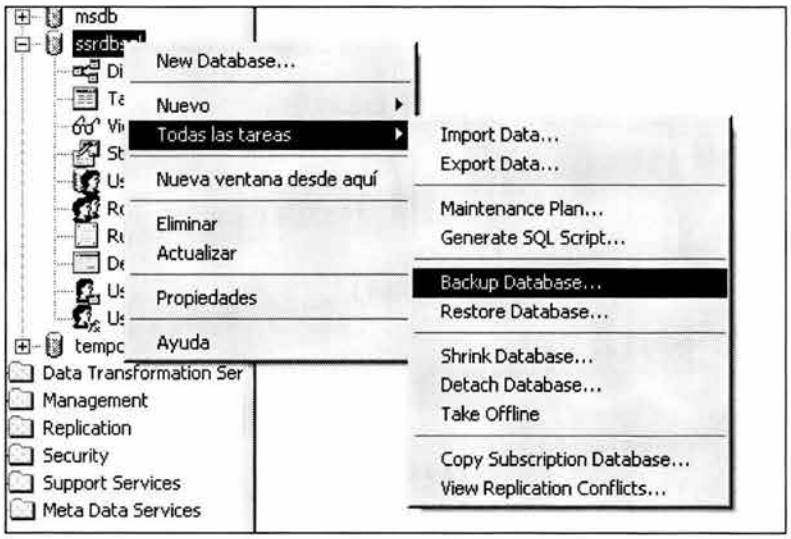
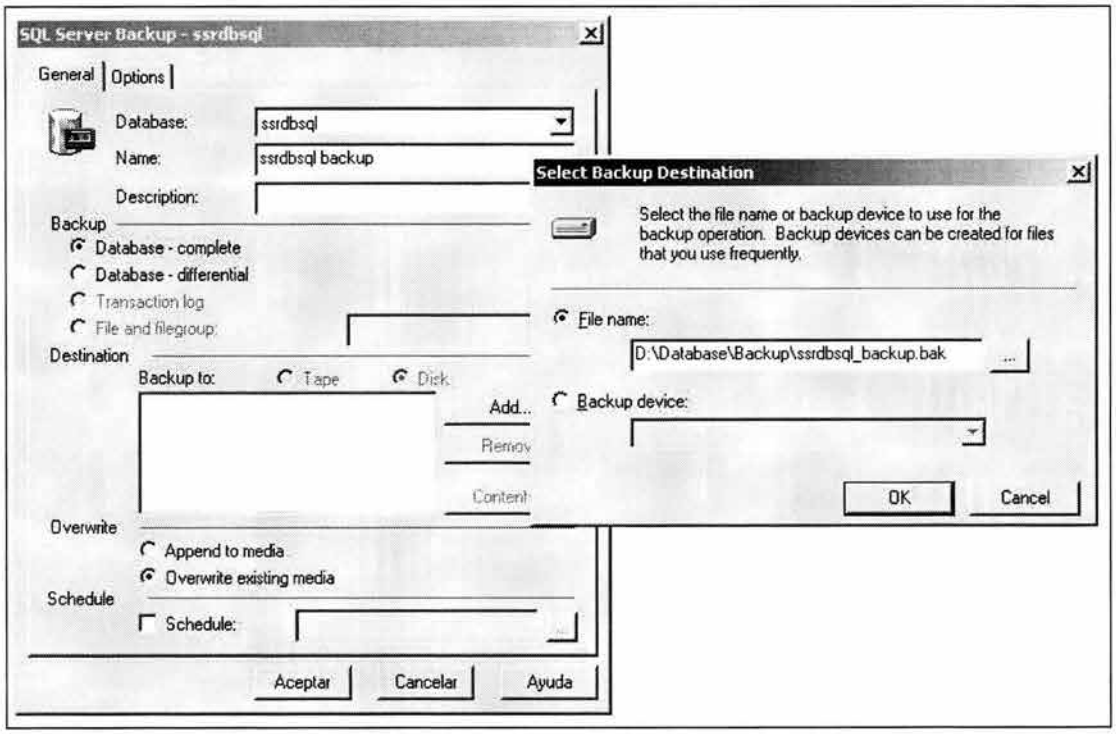


Figura 2.1.1 Ejecución de un respaldo a la base de datos.

Una vez que se selecciona la opción, se presenta un cuadro de diálogo para respaldos, en cual se debe agregar un destino al respaldo de la base de datos que se está generando, mediante un clic en el botón *Add* y aceptando las opciones marcadas de forma predeterminada. Se debe especificar el nombre del archivo que contendrá en respaldo, por ejemplo, el nombre de la base de datos, una palabra descriptiva y la extensión .bak, además de indicar que se sobrescriba cualquier archivo existente. La figura 2.1.2, muestra la interfaz de usuario para este proceso.



2.1.2. Cuadro de diálogo para la realización de un respaldo.

Una vez especificados estos parámetros se aceptan ambos cuadros de diálogo, y el sistema generará el respaldo en el directorio especificado. Al terminar se recibe un mensaje como el de la figura 2.1.3.

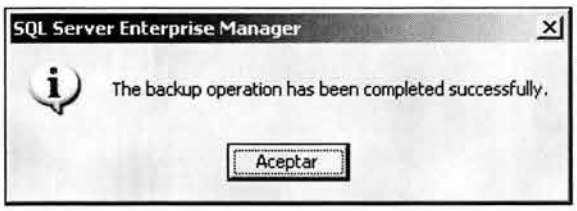


Figura 2.1.3 Respaldo de la base de datos terminado.

2.3 Restauración de un respaldo de la base de datos

En la figura 2.1.1 existe también una opción en el menú contextual de la base de datos llamado *Restore Database* que debe seleccionarse para restaurar la información. Al seleccionar esta opción, se obtiene el cuadro de diálogo para restaurar la base de datos como el de la figura 2.3.1.

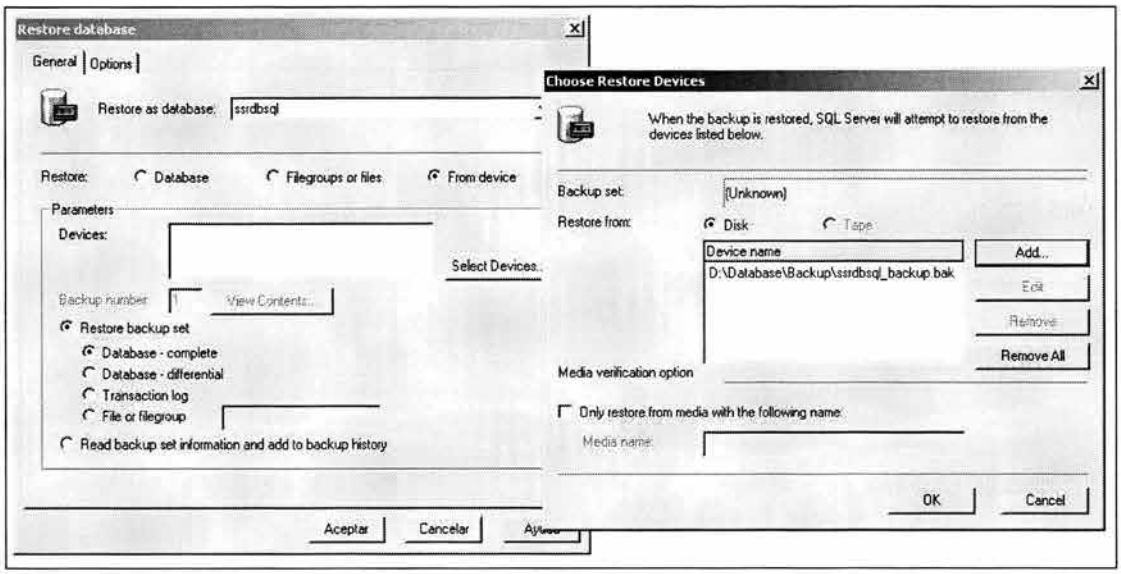


Figura 2.3.1 Restauración de la base de datos.

Se debe elegir la opción *From Device* y al presionar el botón *Select Devices* agregar el archivo que corresponde al respaldo de la base de datos que se hizo con anterioridad. Al especificar esta opción, seleccionamos restaurar la base de datos completa, mediante un clic en la casilla *Database – complete*. Es muy importante saber que cuando se restaura la base de datos, se sobrescriben todas las tablas de la base de datos sobre la que será ejecutado. El sistema informará cuando la restauración termine con un mensaje similar al presentado para el respaldo terminado.

2.4 Automatización de respaldos

Microsoft SQL Server 2000 ofrece la opción de respaldar automáticamente la base de datos, mediante la creación de una tarea que lo realice y que se incluye en un plan de mantenimiento de la base de datos. Este respaldo se ejecuta periódicamente y de forma automática, pudiendo ser diario, semanal o cada determinado tiempo, según sea especificado.

Es muy recomendable este tipo de plan de mantenimiento, para asegurar que independientemente de las actividades que tenga asignadas el administrador, éste se ejecute.

2.5 Control del servicio de SQL Server

Cuando SQL Server se encuentra ejecutando en el servidor, se levanta un servicio llamado MSSQLServer, que puede ser detenido, arrancado o pausado de forma manual. En el caso del servidor que provee la base de datos al sistema, inicia automáticamente al iniciar el sistema, sin embargo, en caso de requerir detenerlo o arrancarlo, se hace mediante el Administrador de Servicios de SQL Server, que se accede mediante un doble clic al icono colocado junto al reloj en la barra de tareas. En la figura 2.5.1 se muestra este administrador.

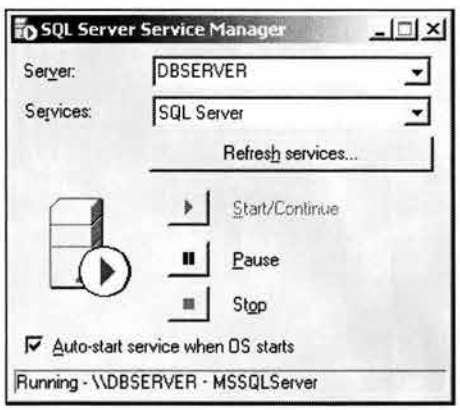


Figura 2.5.1 Administrador de Servicios de SQL Server

CONCLUSIONES

Se cumplió con el objetivo planteado originalmente para el desarrollo de este trabajo, el cual lleva a la automatización de procesos relacionados con el departamento de seguridad de la empresa. El sistema desarrollado es capaz de llevar el control de los inventarios de equipos y usuarios, así como de los incidentes de seguridad que son reportados al área para su atención. El desarrollo del sistema proporciona ahora, seguridad en la información, agilidad en la atención a incidentes, así como en los procesos que involucran a cualquier inventario de dispositivos de la red.

El desarrollo del sistema de control de inventarios de equipos, usuarios e incidentes de seguridad, cumplió con la finalidad principal de automatizar procesos realizados por el área de seguridad que consumían mayor tiempo y que en algunas ocasiones generaban errores o duplicación de información.

La culminación de este proyecto nos permite mostrar la experiencia adquirida en años de trabajo con la cual aportamos lo mejor de nosotros para nuestro desarrollo profesional y el desarrollo mismo de la empresa en la que laboramos.

El trabajo por objetivos permite distribuir las cargas en el equipo de acuerdo a la experiencia y al conjuntar éstas da como resultado la obtención de los objetivos planteados al inicio.

A través de este trabajo, se consiguió un objetivo, por el cual ofrecemos una solución más efectiva consecuencia del trabajo coordinado de todo el equipo, y debido a que la aportación de ideas y cargas de trabajo están orientadas al cumplimiento de una misma meta.

La FI de la UNAM nos forma profesionalmente para competir laboralmente en un mercado que se torna cada día más exigente dado el avance diario de la tecnología.

La modularidad de nuestro mapa curricular nos permite aplicar íntegramente la aportación técnica que cada una de nuestras materias nos ha brindado a lo largo de nuestra carrera.

Al cubrir este mapa curricular de carrera exitosamente, se han obtenido los fundamentos que permiten el desarrollo profesional con una visión emprendedora y de innovación en los diferentes ámbitos de desarrollo.

La actualización tecnológica que podemos obtener posterior a la formación de ingeniería obtenida en la licenciatura es clave para posicionarnos en un nivel competitivo dentro del mercado laboral, ya que aplicando todos los conocimientos adquiridos a lo largo de la carrera es posible tener una mejor comprensión de las tecnologías de información que van surgiendo.

La formación obtenida nos permite elaborar cualquier tipo de proyecto informático por complejo que sea.

BIBLIOGRAFÍA

Libros consultados

- Enciclopedia de Microsoft VB 6.0
  Autor: Francisco Javier Cevallos
  Editorial: Alfa Omega

- Programación avanzada con Microsoft VB 6.0
  Autor: Francesco Balena
  Editorial: Mc Graw Hill

- ASP: Active Server Pages
  Autor: Jesús Bobadilla, Alejandro Alcocer
  Editorial: Mc Graw Hill

- Ingeniería de Software
  Autor: Eric J. Braude
  Editorial: Alfaomega
  México, 2003

- UML y Patrones
  Autor: Craig Larman
  Editorial: Prentice Hall
  España, 2002

Direcciones de Internet

- http://www.pro-3.com.mx/artbas.htm
  Artículo: La arquitectura de las aplicaciones.

- http://www.sybase.com
  Artículo: Sybase Power Builder 8.0.

- http://community.borland.com
  Artículo: A Comparison of Client/Server Development Tools; PowerBuilder vs. Delphi.

- http://dev.mysql.com/tech-resources/crash-me.php?res_id=390
  Artículo: A Comparison of MySQL, SQL Server 2000 and Oracle-9i.

- http://mixteco.utm.mx/~mmoreno/mixteco/IS5.ppt%20[Read-Only].PDF
  Artículo: Verificación y validación. Pruebas de verificación, pruebas de validación y verificación formal.

- http://www.megaone.com/hectorm79/prueba_de_caja_negra.htm
  Artículo: Prueba de caja negra.

- http://www.tecno275.com.ar/articulo6.htm
  Artículo: Conceptos de normalización.

- http://www.fit.um.edu.mx/saulohdz/mcc-ingsoftware/parte4-2.pdf
  Artículo: Diseño de software. Tipos de mantenimiento.

- http://www.microsoft.com/sql/default.asp
  Artículo: Microsoft SQL Server.

- http://mit.ocw.universia.net/curso11208/11/11.208/IAP02/lecture-notes/lecture5-2.html
  Artículo: Diseño de bases de datos relacionales: principios básicos de diseño

- http://usuarios.lycos.es/cursosgbd/UD4.htm
  Artículo: Diseño de bases de datos relacionales.

Buscadores

- http://www.google.com.mx
  Descripción: Google México

- http://mx.yahoo.com
  Descripción: Yahoo México

- http://www.yahoo.com
  Descripción: Yahoo

- http:// www.lycos.es
  Descripción: Lycos