

Escuela Superior Politécnica del Litoral

Facultad de Ingeniería Eléctrica y Computación

Materia :

TOPICO DE GRADUACION II

Proyecto:

**Sistema de control de acceso al Laboratorio
de Computación**

Autores:

Castillo Coronel Pedro
Castro González José
del Salto Valle Leopoldo
Jiménez Falconi Francisco
Malta Mosquera Jessica
Mora William

Moreno Riofrío Alex
Ocampo Barragán Marcelo
Pérez Hernández Jesús
Togra Alvarado Javier
Torres Manzo José
Yépez Pérez Paola

12 de Diciembre de 1996

AGRADECIMIENTO

Primeramente a Dios porque sin la ayuda de el este proyecto jamas se hubiera terminado. En segundo lugar a nuestros padres por todo el apoyo que siempre nos dieron. A nuestros profesores porque además de inculcarnos su conocimiento fueron ejemplos de profesionalismo. Al Ingeniero Guido Caicedo, director del Tópico por su ayuda y colaboración para la realización de este trabajo.



.....

ING. GUIDO CAICEDO ROSSI

DECLARACION EXPRESA

“La responsabilidad por los hechos, ideas y doctrinas expuestos en este documento, nos corresponden exclusivamente; y, el patrimonio intelectual de la misma, a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL”.

INDICE

INDICE.....	V
I. GENERALIDADES DEL SISTEMA.....	1
1.1. ANTECEDENTES.....	1
1.2. OBJETIVOS.....	1
1.3. DEFINICION DEL PROBLEMA.....	2
1.4. JUSTIFICACION DEL SISTEMA.....	3
II. DISEÑO GENERAL DEL SISTEMA.....	5
III.- MODULO DE ACCESO.....	10
3.1. FUNCIONES.....	10
3.2. FUNCIONALIDADES ADICIONALES A LOS REQUERIMIENTOS.....	12
3.3. RESTRICCIONES DE HARDWARE Y SOFTWARE.....	12
3.4. DISEÑO.....	13
3.5. CIRCUITOS DE CONEXIÓN.....	15
3.5.1. <i>Conexión con la cerradura.....</i>	<i>15</i>
3.5.2. <i>Conexión con la Lectora.....</i>	<i>20</i>
3.6. CLIENTE DE AUTORIZACIÓN.....	28
3.7. SERVIDOR DE CONTROL DE LA PUERTA.....	30
3.8. PROCESO FUERA DE LINEA.....	34
3.9. ESTRUCTURA DE ARCHIVOS UTILIZADOS.....	36
3.10. INSTALACIÓN Y CONFIGURACIÓN.....	39
3.10.1. <i>Instalación Desde El Programa De Setup.....</i>	<i>39</i>
3.10.2. <i>Instalación Manual De Los Archivos.....</i>	<i>39</i>
IV. MODULO DE TRANSACCIONES.....	41
4.1. FUNCIONES DEL SERVIDOR.....	41
4.2. FORMATO DEL MENSAJE.....	42
4.3. INSTALACIÓN Y CONFIGURACIÓN.....	45
4.4. DISEÑO DEL SISTEMA DE ARCHIVOS.....	47
V. SISTEMA DE ADMINISTRACIÓN (SERVIDOR).....	50
5.1. FUNCIÓN.....	50
5.2. DISEÑO E IMPLEMENTARON.....	50
5.2.1. <i>Clientes A Los Cuales Brinda Servicio.....</i>	<i>51</i>
5.2.2. <i>Facilidades Proporcionadas En El Programa De Administración.....</i>	<i>51</i>
5.2.3. <i>Seguridad Y Autenticación.....</i>	<i>52</i>
5.2.4. <i>Mecanismo De Consultas.....</i>	<i>52</i>
5.3. ARCHIVOS USADOS EN EL SISTEMA ADMINISTRATIVO.....	55
5.3.1. <i>Introducción.....</i>	<i>55</i>
5.3.2. <i>Archivo Usuarios.....</i>	<i>55</i>
5.3.3. <i>Archivo Grupos.....</i>	<i>55</i>
5.3.5. <i>Archivo Diario.....</i>	<i>57</i>
5.3.6. <i>Archivo Conectados.....</i>	<i>57</i>
5.3.7. <i>Archivo Histórico.....</i>	<i>58</i>
5.3.8. <i>Archivo Eventos.....</i>	<i>59</i>
5.3.9. <i>Archivo Config.....</i>	<i>60</i>
5.3.10. <i>Relación Entre Los Archivos.....</i>	<i>60</i>
5.4. FORMATO DE MENSAJES.....	61
5.4.1. <i>Mensajes De Ingreso , Consulta Y Modificación De Archivos.....</i>	<i>61</i>
5.5. COMPILACION , INSTALACION Y CONFIGURACION.....	69

VI. SERVIDOR PCNFSD	72
6.1. FUNCIÓN.....	72
6.1.1. <i>Autenticación y Seguridades del Sistema</i>	72
6.1.2. <i>Soporte para compartir impresora</i>	73
6.1.3. <i>Determinando Versión de rpc.pcnfsd</i>	74
6.1.4. <i>El log wtmp</i>	74
6.1.5. <i>Llevando rpc.pcnfsd a otros servidores NFS</i>	75
6.2. PROCEDIMIENTO Y MODIFICACIONES REALIZADAS.....	76
6.3. MANEJO DE ARCHIVO.....	77
6.4. INSTALACION Y CONFIGURACION.....	79
VII. CLIENTE DE CONTROL DE TIEMPO	82
7.1. FUNCIÓN.....	82
VIII. CLIENTE ADMINISTRADOR	84
8.1. FUNCIÓN.....	84
8.2. DISEÑO.....	84
8.2.1. <i>Programa de Configuración</i>	84
8.3. PROGRAMA CLIENTE ADMINISTRADOR.....	86
8.3.1. <i>Administración: Cambiar Clave</i>	87
8.4. CONTROL DE LA PUERTA.....	94
8.4.1. <i>Puerta: Abrir la Puerta</i>	94
8.4.3. <i>Puerta: Desbloquear la Puerta</i>	95
8.5. EDICIÓN, CREACIÓN Y ELIMINACIÓN DE USUARIOS Y GRUPOS.....	96
8.6. TRABAJO CON GRUPOS.....	101
IX. SISTEMA DE ARCHIVOS	104
9.1. INTRODUCCIÓN.....	104
9.2. ARCHIVO USUARIOS.....	104
9.3. ARCHIVO GRUPOS.....	105
9.4. ARCHIVO DE ADMINISTRADORES.....	105
9.5. ARCHIVO DIARIO.....	105
9.6. ARCHIVO HISTORIA.....	106
9.7. ARCHIVO EVENTOS.....	107
9.8. ARCHIVO CONECTADOS.....	107
9.9. VARIOS.....	108
CONCLUSIONES Y RECOMENDACIONES	109
CONCLUSIONES.....	109
RECOMENDACIONES.....	109
APENDICES	110
A.- MANUAL DEL USUARIO DEL CLIENTE ADMINISTRATIVO	110
BIBLIOGRAFIA	133

I. GENERALIDADES DEL SISTEMA

1.1. ANTECEDENTES

Los directivos de la facultad de ingeniería eléctrica desean modernizar el laboratorio de computación, haciendo uso eficiente de los equipos que éste posee, tener mayor control sobre las personas autorizadas para acceder al laboratorio y utilizar los mismos, y administrar equitativamente el tiempo de uso de las computadoras para cada estudiante.

Se ha propuesto al grupo de estudiantes del tópico de TCP/IP e INTERNET, realizar un sistema computarizado que mejore el funcionamiento actual de dicho laboratorio.

1.2. OBJETIVOS

Del sistema.

Permitir al administrador del laboratorio:

- Controlar el número máximo de estudiantes permitidos en el laboratorio en un momento dado
- Controlar de forma automática el acceso al laboratorio, permitiendo o negando los requerimientos efectuados por las personas que desean ingresar al mismo.
- No permitir el uso de las computadoras a aquellas personas que no han registrado su ingreso al laboratorio.

- Distribuir de manera controlada el tiempo de uso de las computadoras entre las personas autorizadas para hacerlo.
- Registrar los eventos de ingreso al laboratorio de cada persona autorizada y de uso de las computadoras del laboratorio, para la realización de posteriores consultas.
- Reportes
 - Usuarios Conectados
 - Ingresos al Laboratorio de Hoy
 - Ingresos al Laboratorio por fecha
 - Ingresos al Laboratorio por Usuario
 - Eventos Administrativos
 - Accesos por Máquina

Del proyecto.

Permitir a los desarrolladores:

- Desarrollar el sistema, aplicando la tecnología cliente - servidor
- Aplicar los conocimientos del protocolo de comunicaciones TCP/IP.

1.3. DEFINICION DEL PROBLEMA.

Actualmente, es poco el control que puede ejercer el administrador, en el acceso de los usuarios al laboratorio, y en el uso de las computadoras.



figura 1.1. Método de utilización de Laboratorio actualmente.

El mecanismo de control y administración implementado es manual, en el cual los ayudantes de turno deben encargarse de asignar las computadoras para los usuarios (ingresar clave de acceso), y al mismo controlar que personas entran y salen del laboratorio. Para un solo ayudante es una carga grande

El registro manual de las asignaciones de computadoras a los usuarios dificulta la ejecución de consultas y reportes de uso de las mismas.

Mediante el sistema actual es muy difícil realizar una distribución equitativa del uso de las computadoras entre los usuarios, para así evitar el monopolio que algunos estudiantes realizan con las computadoras.

1.4. JUSTIFICACION DEL SISTEMA.

El desarrollar un sistema que asista a los ayudantes encargados en la administración de los recurso del laboratorio, brinda las siguientes ventajas:

- Permite definir los usuarios autorizados para ingresar al laboratorio
- Permitir definir los usuarios autorizados para usar las computadoras

- Controla automáticamente el acceso de los usuarios al laboratorio, basado en los permisos establecidos previamente.
- Brinda mayor seguridad al laboratorio, ya que niega el uso de las computadoras a los usuarios que no han registrado su ingreso al laboratorio.
- Para ser implementado no necesita equipos nuevos ni de características especiales, sino que utiliza los ya existentes en el laboratorio.

II. DISEÑO GENERAL DEL SISTEMA

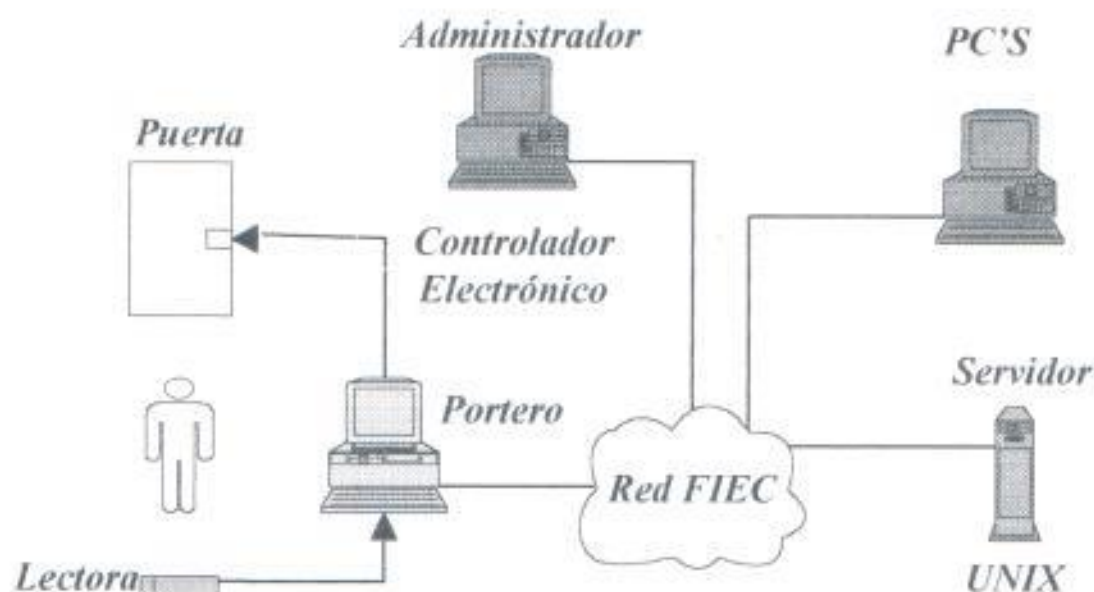


figura 2.1. Diagrama del Diseño General del Sistema

A la resolución del problema propuesto lo que se desea implementar es un control mas estricto sobre el uso del Laboratorio en donde los estudiantes habilitados por medio de una tarjeta magnética u otros usuarios especiales sean estos profesores u personas autorizadas que no tengan tarjeta tenga un tiempo limitado o ilimitado para el uso del computador y una vez concluido el tiempo del mismo el sistema se apague automáticamente. Esto permitirá que el ayudante u otro administrador no se encuentre constantemente vigilando el tiempo de conexión de otro usuario lo que le permitirá realizar otras actividades relacionadas a su trabajo.

El sistema para su efecto se divide en tres módulos especiales que son los siguientes:

1. Modulo de Acceso
2. Modulo de Transacciones

3. Modulo de Administración

Cada uno de los módulos será explicado detalladamente en su capítulo correspondiente aquí explicaremos en forma general lo que el sistema realiza:

Un usuario habilitado pasa una tarjeta a través de la lectora este revisara un archivo en donde se encuentran todos los usuarios habilitados y que tengan tiempo de máquina para permitirles el ingreso dentro del laboratorio, el ingreso al Laboratorio no implica necesariamente el uso de el tiempo disponible, el usuario primero debe ingresar a una PC con su usuario y clave respectiva para que el tiempo le empiece a correr, si el usuario se halla trabajando en modo Windows 3.1 o Windows 95 el sistema le mostrara un reloj que le indicara el tiempo disponible que le queda, si en caso se encontrara en modo DOS el ayudante o administrador debe estar al tanto de que el usuario salga cuando el tiempo le ha expirado, es importante hacer notar que una vez que un usuario ha ingresado con su usuario y clave no lo puede hacer desde otra PC es decir que solo puede haber un usuario por máquina.

En caso de-que exista un usuario especial que no tenga tarjeta pero que necesita ingresar al Laboratorio con su respectiva autorización el ayudante o Administrador se encuentra en la facultad de abrirle la puerta automáticamente

Si en un momento dado el servidor principal(UNIX) se encontrara deshabilitado existe una base de datos de usuarios en el servidor que realiza la función de portero para permitir el ingreso de los usuarios dentro del Laboratorio, aunque no podrán usar el sistema hasta que el servidor Unix sea nuevamente habilitado.

Si un usuario se encuentre bloqueado así tenga la tarjeta magnética el sistema no le permitirá ingresar al Laboratorio.

Un administrador puede también volver a dar mas tiempo a un usuario si fuera necesario como es el caso de que el Laboratorio se encuentre vacío o que sea un usuario especial al cual hay que darle mas tiempo de máquina.

Si un usuario que no tiene tiempo de maquina pero que se encuentre dentro del Laboratorio y trata de ingresar a una PC, su requerimiento será rechazado y no podrá ingresar a la PC.

El sistema también permite llevar un control de las máquinas al determinar cuales son los usuarios que la utilizaron en un día determinado, con ello en caso de daño se sabrá las personas que utilizaron por ultima vez dicho computador.

También se puede llevar un control de los administradores en donde se podrá determinar las acciones que ellos realizaron durante el día o fecha dada.

DIAGRAMAS DE APLICACIONES

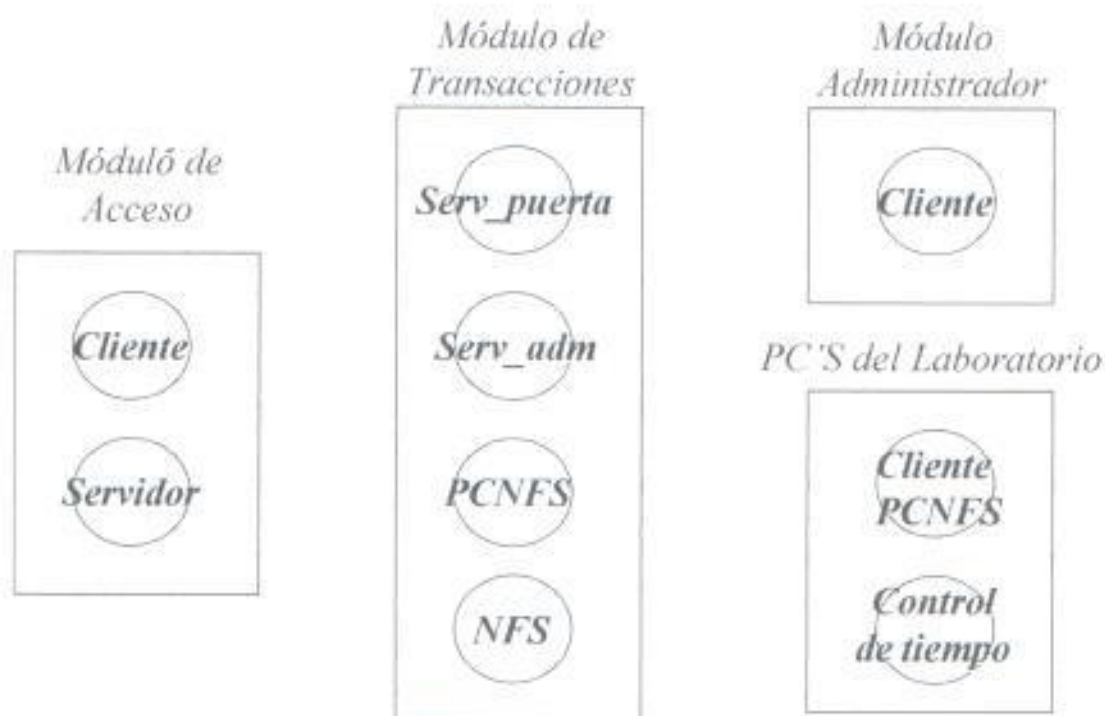


Figura 2.2. APLICACIONES DESARROLLADAS POR CADA MODULO REALIZADO.

Para el desarrollo de cada uno de los módulos se tuvo que implementar ciertos servidores con sus respectivos clientes.

El diagrama muestra en detalle las aplicaciones que se desarrollaron por módulos en donde podemos ver que:

1. **Modulo de Acceso:** Es el que permite el ingreso del usuario a través de la puerta y se encuentra dividido en 1 servidor de acceso y en un cliente de acceso.
2. **Modulo de Transacciones:** Es el corazón del proyecto todas las acciones realizadas por los otros módulos deben interactuar con este módulo. Por su complejidad tuvo que dividirse en 2 servidores uno para el control de acceso y otro para las tareas administrativas, a la vez que se trabajo sobre la plataforma NFS ya montada, y sobre el servidor PCNFS que se modifico para permitir controlar acceso de un usuario y que se encuentre habilitado en capitulos posteriores se explicara con mas detalle.
3. **Modulo de Administración:** Es la parte visible del sistema es el que interactua mas estrechamente con el modulo de transacciones y permite realizar tareas de tipo administrativa como es el control de usuarios y generación de reportes, asi como también el bloqueo y desbloqueo de la puerta. Consistia básicamente de un único cliente.

4. Clientes en la PC : En las Pe para poder acceder a la misma y poder cargar los archivos de configuración suficientes debía contener un cliente PCNFS, el cual montaba las unidades del servidor UNIX las cuales contenían los archivos necesarios para poder utilizar el PC. Así mismo se debía instalar un cliente de control de tiempo en las máquinas, para que una vez terminado el tiempo disponible bootee el computador para que el usuario no la pueda seguir usando y permitir que otro pueda ingresar.

III.- MODULO DE ACCESO

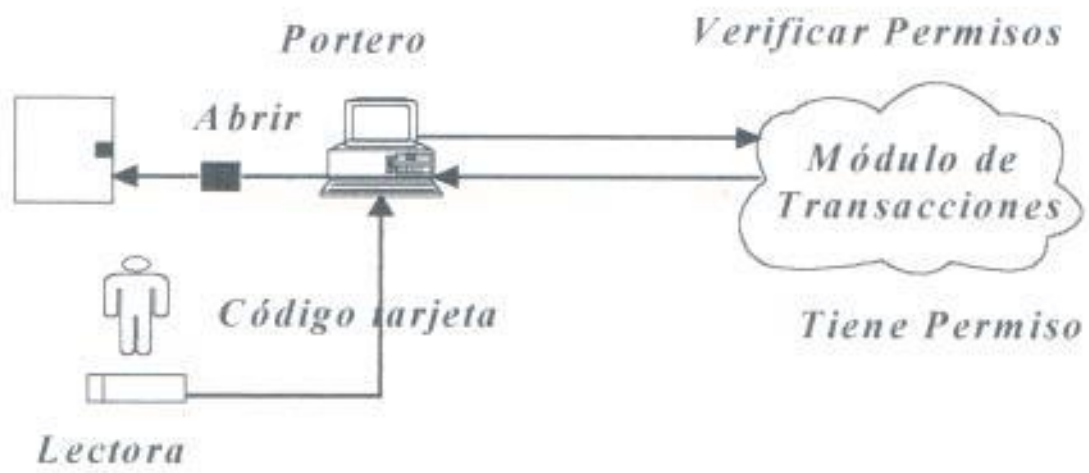


figura 3.1 Esquema del Módulo de Acceso.

El módulo de acceso es el encargado de permitir el acceso de los estudiantes, profesores u otros usuarios dentro del Laboratorio a través de una lectora de tarjetas magnéticas siempre y cuando se tengan los permisos necesarios o a través de un requerimiento especial que permita al administrador abrir la puerta sin necesidad de la lectora.

3.1. Funciones

El presente módulo forma parte de un sistema integrado de administración de utilización de los equipos del Laboratorio de Computación de la Facultad de Ingeniería Eléctrica ; y se encargará de realizar las siguientes funciones:

- Controlará el acceso de los estudiantes al laboratorio. Mediante el uso de una tarjeta con banda magnética, el estudiante podrá identificarse con el sistema pasando la tarjeta por una lectora conectada a una computadora.
- Validará que el estudiante que pasa la tarjeta por la lectora esté autorizado a ingresar al laboratorio y de ser así automáticamente abrirá la puerta de ingreso.
- Se deberá registrar el ingreso de todos los estudiantes, de manera que quede almacenada información que luego pueda ser procesada para obtener resultados estadísticos.
- Debe haber una opción que permita abrir la puerta directamente desde el mismo computador y también desde un computador diferente del que se encuentra corriendo el sistema.
- Debe considerarse un plan de contingencia que permita que el sistema de control de ingreso continúe funcionando "off-line" en caso de ocurrir una falla en la red del laboratorio.
- Utilizará bajos recursos de hardware y software, ya que el equipo donde se va a ejecutar será una máquina dedicada que no podrá ser utilizada por los estudiantes y por lo tanto no debe disminuir los equipos nuevos que se encuentran disponibles.
- Debe funcionar utilizando la arquitectura cliente-servidor, sobre una red con protocolo TCP-IP y como mecanismo de comunicación debe utilizar sockets.
- Implementará una opción que permita el bloqueo lógico de la puerta, de tal manera que cuando se encuentre en este estado no pueda ser abierta desde el sistema.

3.2. Funcionalidades Adicionales A Los Requerimientos.

- Implementación de un mecanismo de autenticación que evite que lleguen requerimientos de abrir la puerta desde cualquier otro programa distinto al definido dentro del sistema.
- Utilización de un interruptor que permita accionar la cerradura directamente, sin intervención del sistema.

3.3. Restricciones de Hardware y Software.

A continuación se detallan los requerimiento mínimos que se necesitan para el normal funcionamiento del subsistema de Control de Acceso.

- Hardware
 - Procesador 386 16 MHz ó superior
 - 4 Mb RAM
 - Tarjeta de red
 - 2 puertos seriales
 - Lector serial de banda magnética
 - Circuito electrónico para controlar la cerradura
 - Interruptor eléctrico
 - Botador eléctrico
 - Transformador 24 Vac
- Software

- DOS versión 3.3 ó superior
- Windows 3.1 ó superior
- Driver para tarjeta de red
- Trumpet 2.0 ó superior
- Visual Basic 3.0 Professional Edition

3.4. Diseño

El módulo de Acceso para cumplir los requerimientos se divide en cuatro componentes funcionales que van a cumplir tareas específicas e independientes :

- Circuitos de conexión
- Cliente de autorización
- Servidor de control de la puerta
- Proceso fuera de línea



Figura 3.2. Componentes del Módulo de Acceso

Todos los componentes, excepto el primero, utilizan procesos de comunicación a través de la red. Esta comunicación como fue definida en los requerimientos, se la hace utilizando el protocolo IP en la capa de red y TCP como protocolo de transporte por sus características de confiabilidad, recuperación de errores y su característica de ser orientado a conexión.

El protocolo de mensajes implementado entre el cliente y el servidor utiliza datos en formato carácter por simplicidad y teniendo en cuenta que la cantidad de datos transmitida es bastante reducida.

3.5. Circuitos De Conexión

El computador necesita utilizar dos circuitos para conectarse a cada uno de los dispositivos desde los puertos seriales. Se necesita un circuito electrónico para conexión con la cerradura eléctrica y un circuito para la conexión con la lectora de banda magnética.

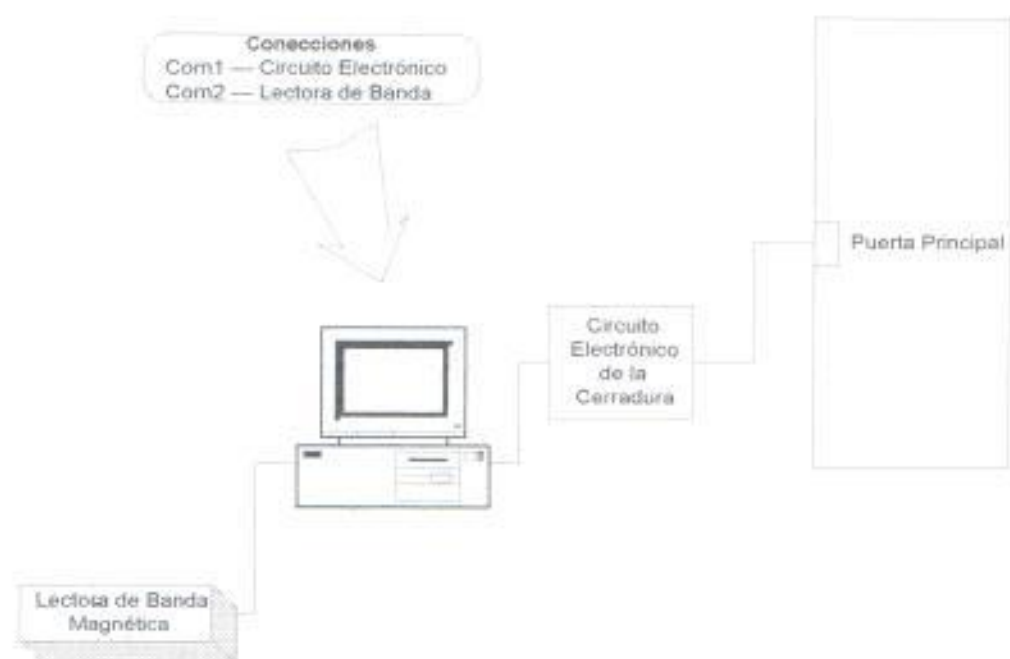


Figura 3.3. Circuito de Conexión

A continuación detallamos los 2 circuitos de conexión que pueden ser implementados:

3.5.1. Conexión con la cerradura.

Actualmente en el mercado existen 2 sistemas de cerradura eléctricas:

Chapas eléctricas

Botadores eléctricos

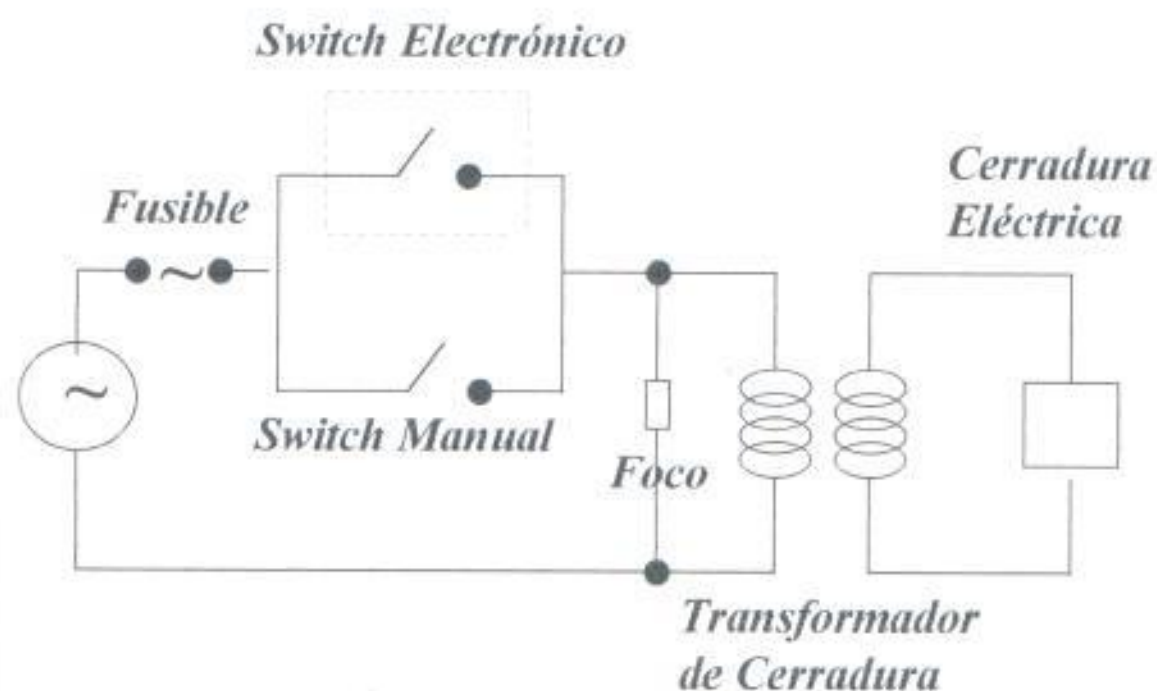


Figura 3.4. Circuito de la Cerradura

Las chapas eléctricas, es una chapa completa con activación eléctrica y llave para los momentos en que no hay energía eléctrica, necesitan de un transformador que puede ser de 9 o 12 Vac, este transformador se lo puede comprar aparte o se puede utilizar el transformador de otro equipo que ya se esté utilizando, como el portero eléctrico. Es importantísimo en este sistema seleccionar correctamente si la puerta necesita una chapa derecha o una chapa izquierda, ya que no son intercambiables.

El botador eléctrico, este es una adaptación para chapas de pomo normales que se desea convertir a eléctricas, en este sistema únicamente se incluye el enclavamiento para el pestillo que se instala en el batiente, y justamente este enclavamiento el que funciona eléctricamente. También necesita de un transformador, generalmente de 24 Vac, que se puede comprar aparte o se puede utilizar uno de otro equipo.

Entre estos sistemas existen dos diferencias principales: el modo de abrir la puerta y sus costos.

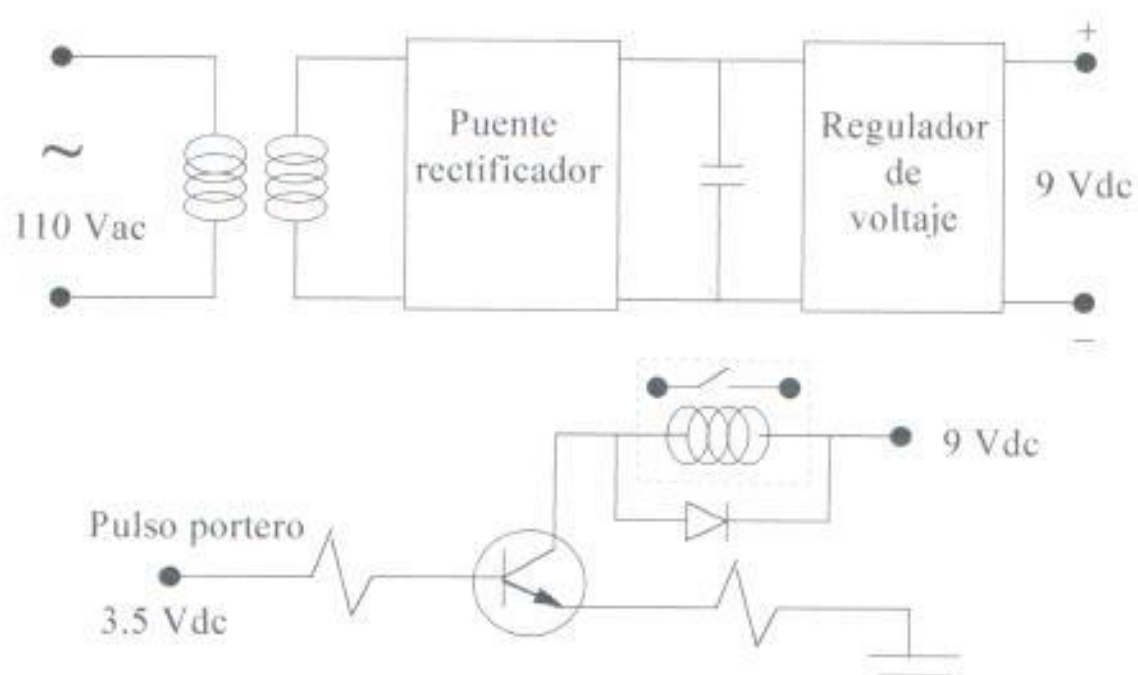
La chapa eléctrica una vez accionada deja la puerta abierta y la persona puede entrar o en caso contrario la puerta se quedara abierta. El botador eléctrico libera el pestillo de la chapa únicamente mientras este siendo accionado, entonces la persona tiene que empujar la puerta durante ese instante o de lo contrario el botador volverá a enclavarse y la puerta quedara cerrada; en este caso si la persona no entra la puerta quedara cerrada.

Finalmente se escogió el sistema de botador eléctrico por su bajo costo, porque no requiere hacer un cambio de cerradura sino que hace uso de la ya instalada en la puerta del laboratorio, no requiere cambiar de llaves ni sacar copias de nuevas llaves que tengan que distribuirse entre el personal de la ESPOL, e incluso el hecho de que la puerta tiene que empujarse para abrirse, ayudara a que la puerta no quede abierta inadvertidamente.

Interruptor manual

Este interruptor podrá instalarse en cualquier lugar del laboratorio y esta conectado en paralelo con el circuito electrónico que hace de interruptor.

Interruptor electrónico



Capacitor: 470 μ F a 50 V

Puente Rectificador : PT - 95126

Regulador de Voltaje: 7809 C

Resistencia de Entrada : 39 OHMIOS

Resistencia de Salida : 47 Ohmios

Relay : 2115A DOO5 - M

Figura 3.5. Interruptor electrónico

Cabe resaltar que el circuito que se ha diseñado se conecta antes del transformador del botador y por lo tanto es independiente de la cerradura eléctrica, del transformador, marca de la chapa, etc. El mismo circuito funcionara con cualquier modelo de cerradura.

El corazón del circuito es un relay de 5Vdc, es importante escoger el voltaje del relay, el cual depende del circuito que se construya, en nuestro caso son voltajes TTL. Nótese que el relay no es de 110Vac, son lo contactos del relay que permiten el paso de los 110Vac y la corriente respectiva.

Para energizar el relay se utiliza un transistor, el cual es saturado con la señal que envía el computador para abrir la puerta, en este momento el relay cierra sus contactos normalmente abiertos y cierra el camino que lleva la corriente al transformador del botador eléctrico. Finalmente el transformador activa el botador, este libera el pestillo de la chapa de pomo y la puerta puede abrirse.

Se ha conectado en paralelo con el relay un diodo, cuya función es protegerlo de las corrientes que la bobina tiene a almacenar después de desenergizar el circuito.

3.5.2 Conexión con la Lectora

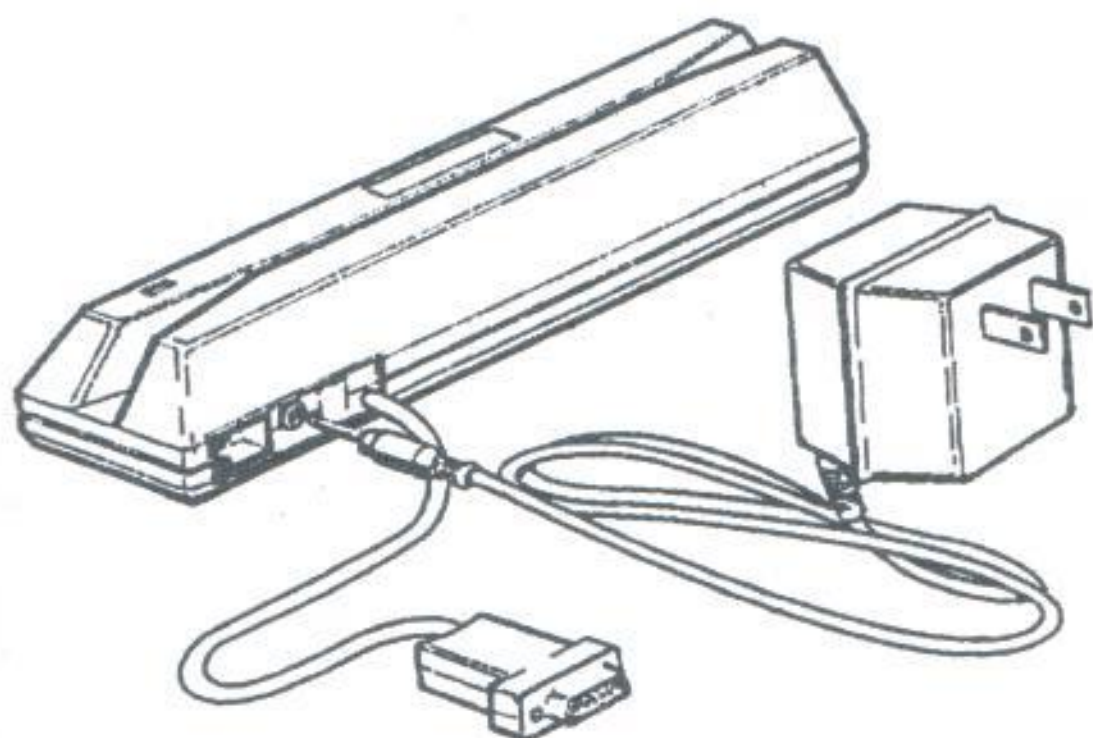


Figura 3.6. Lectora de Tarjeta Magnética

Especificaciones de la lectora de banda magnética a utilizarse

Marca : - MAGTEK

Modelo : MT - 211232

Especificación física

Color : Beige

Dimensiones : 6 ½" de largo x 1 ¾" de Ancho x 1 5/8" de altura

Peso : Lector : 7 oz. Adaptador : 11oz.

Req. de Volt. : 9 Voltios

Formato de Mensaje : ASCII

Velocidad :	3-125 IPS a 75 BPI
Conector :	9 pines hembra, requiere un cable de interfase

El MT-211232(disponible en ambas pistas única y doble) lee datos codificados sobre tarjetas de cintas magnéticas que siguen los estándares ANSI (AMERICAN NATIONAL STANDARD INSTITUTE) e ISO (INTERNATIONAL STANDARD ORGANIZATION). La Lectora fácilmente interactúa con un host usando un conjunto de simples comandos. Para transmitir datos la tarjeta magnética al host, tiene 2 diferentes modos de operación (Unbuffered o Buffered) que puede ser seleccionando por el usuario. Dos bloques de conjuntos de switches (Switch Block A y Switch Block B) son localizados en la tarjeta de la lectora del circuito. Estos bloques son usados para seleccionar el modo de operación, los parámetros de comunicación RS-232, y el protocolo de usuario deseado.

Cuando una tarjeta de cinta magnética es pasada a través de la lectora, el mensaje entero es chequeado por errores usando paridad y LRC(la tarjeta magnética debe ser pasada en un continuo camino a través de la lectora para prevenir un error. Cuando un error es detectado la lectora transmite el carácter ASCII "E").

3.5.2.1. Modos De Operación.

Esta es una descripción de los modos de operación y los switch que son requeridos de la lectora para la configuración RS232 .

Modo 1.- Unbuffered

En el modo operativo Unbuffered, los datos desde la lectora es automáticamente enviado al host sin envío de requerimiento. Cuando una tarjeta es pasada a través de la lectora, el dato es transmitido inmediatamente y no es retenido.

La lectora no necesita recibir comandos desde el host con el propósito de transmitir datos. Sin embargo, la lectora responde a un Inquiry Command para enviar un ASCII "R". Por ejemplo, un Inquiry Command puede ser usado para determinar si el power esta ON en un remoto MT-211232.

Modo 2.- Buffered

En el modo operativo buffered, la lectora guarda los datos de la tarjeta en un buffer de memoria y no transmite ningún dato al host hasta que un Inquiry Command es recibido. Al recibir de un Inquiry Command, El dato es transmitido para el host. Si ningún dato esta presente en la memoria buffer, únicamente el ASCII "R" debe ser transmitido. Los datos no son limpiados desde el buffer de memoria hasta que un Release Command es recibido. La lectora no puede leer otra tarjeta hasta que el buffer es limpiado.

Comandos de Lectora para Host

Todo los comandos transmitidos desde el host a la lectora deben ser precedidos por un caracter ASCII "ESCAPE" (ESC). Caracteres que preceden o siguen la secuencia de el comando no afectan la interpretación de comando de la lectora. Todo caracter ASCII debe ser transmitido en UPPER CASE (e.g., ASCII "I" y "R").

B-4 ON <ESC> "I"	Inquiry Command: Requerimiento para la lectora para transmitir dato o error en el modo buffered. transmite un ASCII "R" en el modo unbuffered.
B-4 OFF <ESC> "+"	

B-4 ON <ESC> "R"	Release Command: Requerimiento para la lectora para limpiar la memoria del buffer de algún dato presente. No tiene efecto en el modo Unbuffered.
B-4 OFF <ESC> "."	

3.5.2.2. Conjunto De Bloques De Switches.

2 Bloques de switches, Switch Block A y Switch Block B, son localizados en el circuito board de la lectora MT-211232. Estos bloques de switches, etiquetada SWA y SWB, contiene switches numerados 1-8. Estos switches debe ser seteado mientras el power esta off para asegurar que el switch setting estén apropiadamente cargado.

SWITCH BLOCK A (SWA)

- **Switch 1, 2, 3:** Esto switches setean el ancho de Banda (bits por segundo), o la tasa en la cual los datos es recibidos y transmitidos entre la lectora y el host.
- **Switch 4:** Este switch setea la PARIDAD.
- **Switch 5:** Este switch habilita la PARIDAD.

- **Switch 6:** Esto es un switch opcional que envía el frame de caracteres cuando se teja sobre la posición ON.
- **Switch 7:** Este es un switch que envía el caracter ESCAPE (ESC) cuando se sejea en la posición ON.
- **Switch 8:** Este es un switch opcional que envía el frame de caracteres END OF TEXT (ETX) cuando se sejea sobre la posición ON.

SETEO DE SWITCH POR BAUD RATE

Baud Rate	SW1	SW2	SW3
300	OFF	ON	ON
600	ON	OFF	ON
1200	OFF	OFF	
2400	ON	ON	OFF
4800	OFF	ON	OFF
9600	ON	OFF	OFF
19200	OFF	OFF	OFF

SETEO DE SWITCH PARA CONDICION PARIDAD

Paridad	SW4	SW5	OBS.
ODD	ON	ON	(Paridad Habilitada)
EVEN	OFF	ON	(Paridad Habilitada)
PARIDAD = 1	ON	OFF	(P. Desahabilitada)
PARIDAD = 0	OFF	OFF	(P. Desahabilitada)

SWITCH BLOCK B (SWB)

- **SWITCH 1:** Este es un switch opcional que envía el caracter CARRIAGE RETURN (CR), cuando esta en la posición ON.
- **SWITCH 2:** Este switch setea el modo BUFFERED o UNBUFFERED. Switch 2 debe estar en la posición ON para el modo buffered y OFF si se desea unbuffered.
- **SWITCH 3:** Este Switch es seteado por la fabrica a OFF y no debe ser cambiado.
- **SWITCH 4:** Este switch es seteado por la fabrica a ON para ESC "Y" y ESC "R", OFF para ESC "+", ESC "-".
- **SWITCH 5 y 6:** Estos switches son seteados por la fábrica y no deben ser cambiados.
- **SWITCH 7 :** Localizar switch 7 en la posición ON para implementar las señales de control conjuntas RTS (Request to Send) y CTS (Clear To Send). Si el host es implementado el CTS (Clear to Send), este switch debe ser seteado en la posición OFF.
- **SWITCH 8 :** Localizar en la posición ON implementa las señales de control conjuntas DTR (DATA TERMINAL READY) y DSR (DATA SET READY). Si el host es implementado con la señal de control DSR (Data-Set Ready) este debe estar en la posición OFF.

Seteo de switches para configuración en el Proyecto.

SWITCHES "A"

1 -> ON

2 -> OFF

3 -> OFF

4 -> OFF

5 -> ON

6 -> ON

7 -> ON

8 -> ON

SWITCHES "B"

1 -> OFF

2 -> OFF

3 -> OFF

4 -> OFF

5 -> ON

6 -> OFF

7 -> OFF

8 -> OFF

3.5.2.3. Interfaces Eléctrica

Los siguientes pines son usados cuando la lectora es conectada a un único host o terminal.

PIN No.	Señal	Función
3	TD	Transmitted Data , señal RS-232. Este pin transmite datos desde el MT-211232 al host.
2	RD	Received Data , señal RS-232. Este pin recibe datos enviados desde el Host a la lectora(MT-211232)
7	RTS	Request To Send , señal RS-232. Este pin envía una señal al host para indicar que la lectora esta lista para transmitir datos.

8	CTS	Clear To Send , señal RS-232. Este pin recibe una señal desde el host para permitir que el dato sea transmitido.
6	DSR	Data Set Ready , señal RS232. Este pin recibe una señal desde el host para indicar a la lectora que el host esta activo.
5	GND	Circuito a Tierra
4	DTR	Data Terminal Ready , Señal RS232. Este pin transmite una señal para el host para indicar que el MT-211232 esta activo. (i.e., poder esta encendido)

3.5.2.4. Asignación De Pines Para Puerto Serial

a) Cable de interfase con señales de control

La lectora no esta en modo listo al menos que la PC este lista para aceptar el dato. La PC puede chequear para ver si la lectora esta activa. Los Switch B7 y B8 deben estar OFF.

Reader End	PC End
RXD 2	TXD 3
TXD 3	RXD 2
DTR 4	DSR 6
GND 5	CTS 8
DSR 6	GND 5
CTS 8	DTR 4
RTS 7	CD 1

3.6. Cliente De Autorización

Este componente del subsistema de acceso se encarga del proceso de obtener la identificación del estudiante una vez que pasa la tarjeta por la lectora de banda magnética y a continuación realiza un requerimiento a otro subsistema que contiene un programa servidor que valida que el usuario esté autorizado, enviando una respuesta al cliente. En caso de obtener una respuesta afirmativa se activará el switch electrónico de la cerradura que permitirá abrir la puerta.

A continuación se muestra la máquina de Estado de el cliente de autorización

A continuación se indica la interacción entre el cliente de autorización y el componente **servidor de puerta** del Subsistema Controlador de Sesiones.

Subsistema de Acceso Subsistema de Sesiones

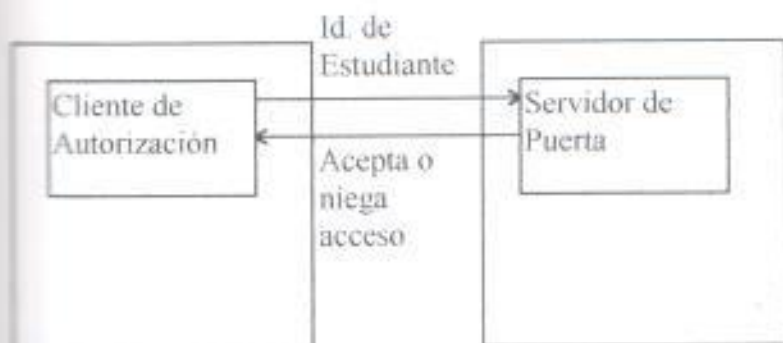


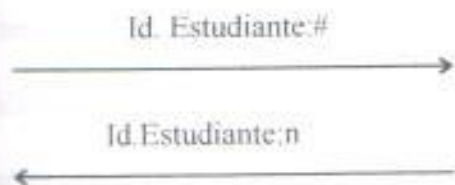
Figura 3.7. Esquema del Cliente de Autorización

En el esquema anterior se detalla el requerimiento que realiza el cliente de autorización al servidor de puerta del subsistema de sesiones. El cliente envía la identificación del estudiante, que para este diseño se consideró que sea el número de matrícula que consiste de siete dígitos y el servidor le envía una respuesta aceptando o negando el requerimiento de ingreso al laboratorio. En caso de que la respuesta sea positiva, el cliente de autorización activará el puerto que controla el circuito de la cerradura para que la puerta se abra, caso contrario el estudiante no podrá ingresar al laboratorio.

Protocolo de Comunicación

Cliente

Servidor



Id.Estudiante = 7 dígitos

= dos puntos y símbolo de número

= Código de retorno (1 dígito):

0: Acceso permitido

1: Estudiante no existe

2: Pertenece a un grupo inactivo

3: Estudiante sancionado

4: No tiene cupo

5: No tiene tiempo en el periodo

6: Comando desconocido)

3.7. Servidor De Control De La Puerta

De acuerdo a los requerimientos, la puerta debe estar en la posibilidad de abrirse respondiendo a un requerimiento desde una máquina distinta a la que corre el subsistema de control de acceso. Para cumplir esta funcionalidad se definió un componente que hace las veces de servidor para procesar los requerimientos de abrir, bloquear y desbloquear la puerta, provenientes de un cliente que es parte del Subsistema de Sesiones. Este servidor adicionalmente maneja un mecanismo de autenticación que evita que cualquier otro cliente diferente al definido para que realice los requerimientos, envíe solicitudes de abrir la puerta. La comunicación se realiza entre el Servidor de control de puerta y el Servidor Administrativo del Subsistema de sesiones.

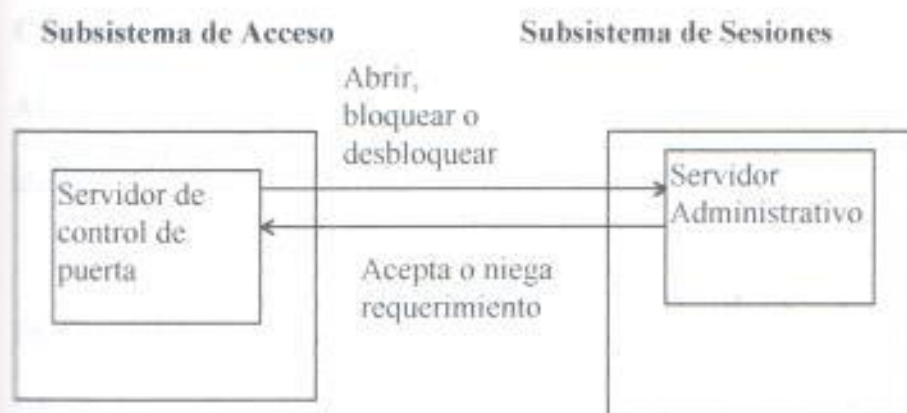
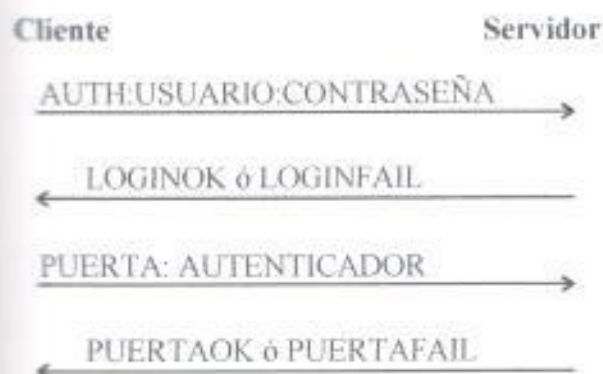


Figura 3.8. Esquema del Servidor Control de la Puerta.

Mecanismo de Autenticación

Se lo implementa utilizando una palabra clave única que aprenden tanto el cliente como el servidor cada vez que se van a comunicar. De esta manera, todos los mensajes que viajen entre cliente y servidor llevarán la clave, asegurando de esta manera que cualquier otro proceso no pueda enviar requerimientos falsos. El proceso de autenticación se lleva a cabo realizando la función de cliente desde el servidor de control de acceso y haciendo requerimientos al Servidor de Puerta en el Subsistema de Sesiones.

Protocolo para Autenticación



USUARIO = Identificación de un usuario que sea administrador o ayudante

CONTRASEÑA = Clave del usuario

AUTENTICADOR = Palabra clave de 10 caracteres alfabéticos generados aleatoriamente

En el primer requerimiento se envía el código del usuario y la clave al servidor del Subsistema de Sesiones, este servidor valida que el usuario y la clave enviados estén correctos, es decir que exista un usuario con ese código y que además la clave enviada coincida con la que tiene el usuario en el sistema. Adicionalmente el servidor verifica que este usuario tenga los derechos de administrador o ayudante. La respuesta a este requerimiento son dos posibles valores: LOGINOK en caso de éxito y LOGINFAIL en caso de fracaso.

Si el primer requerimiento fue exitoso, se envía el segundo, el cual contiene el código autenticador- de diez caracteres alfabéticos aleatorios, la respuesta a este requerimientos es como en el caso anterior dos valores: PUERTAOK en caso de que el proceso de aprendizaje del código autenticador se hizo exitosamente y PUERTAFAIL si ocurrieron errores que no permitieron completar el proceso.

Protocolo del Servidor de Control de la puerta



El servidor para control de la puerta puede recibir tres tipos de requerimientos acompañados del código autenticador generado por el proceso de autenticación explicado anteriormente. El primero de estos requerimientos es el de OPENDOOR el cual se interpreta como un pedido de abrir la puerta, lo cual procederá a hacer el servidor siempre y cuando el código autenticador enviado con el requerimiento coincida con el que él generó inicialmente en el procedimiento de autenticación. A este requerimiento responde con dos posibles valores OPENDOOROK en el caso de que la puerta pueda ser abierta sin ningún inconveniente y retorna OPENDOORFAIL en caso contrario. Para los otros dos requerimientos: LOCKDOOR (bloquear la puerta) y UNLOCKDOOR (desbloquear puerta) el comportamiento es exactamente igual al de OPENDOOR.

Es importante anotar que los procesos de bloquear y desbloquear la puerta son puramente lógicos, en ningún momento la puerta es bloqueada físicamente.

3.8. Proceso Fuera De Línea

Este componente del Servidor de Control de Acceso permite que ciertos procesos del sistema continúen funcionando después de que ocurre una falla en la red, impidiendo de esta manera la comunicación entre los subsistemas.

Para resolver este inconveniente se utiliza un archivo local conteniendo todos los usuarios definidos dentro del sistema. El proceso de autorización de usuarios en lugar de hacer un requerimiento al Servidor de Puerta del Subsistema de Sesiones verifica la existencia del usuario en el archivo local y permite que éste ingrese al laboratorio sólo en caso de que adicionalmente a existir en el archivo también pertenezca al grupo de Administradores o de Ayudantes.

Todos los eventos ocurridos durante el periodo de pérdida de comunicación son registrados en un archivo local que luego de restablecerse la comunicación, es enviado al Servidor de Puerta del Subsistema de Sesiones.

De acuerdo a lo indicado, para realizar este proceso se utilizan dos archivos:

permisos.prt: Contiene los usuarios y permisos

fdl.prt: Contiene los registros de sucesos durante el tiempo de fuera

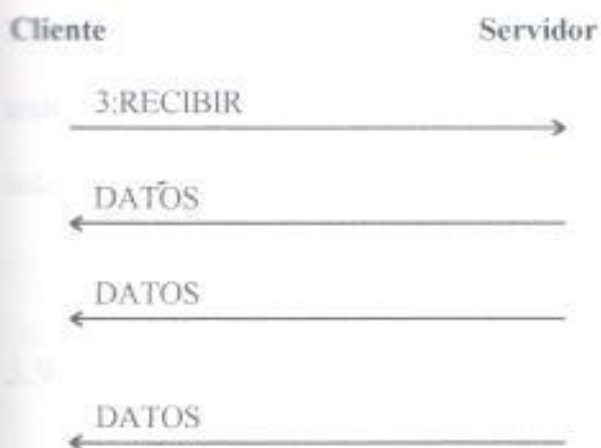
de línea

Se deben ejecutar dos procesos para cumplir el funcionamiento en caso de contingencia:

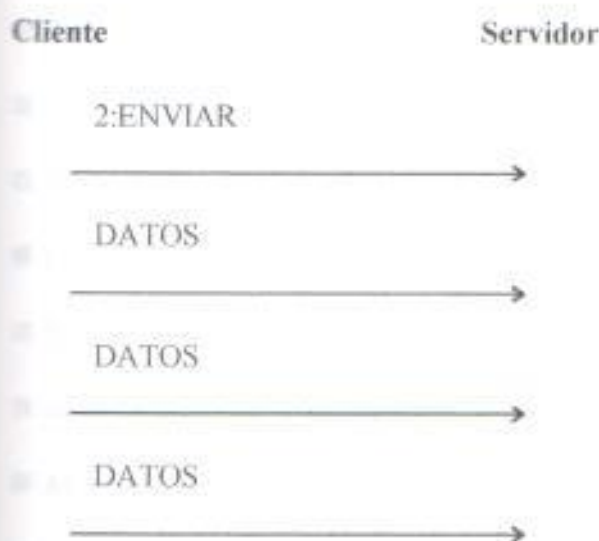
- Transmitir el archivo de permisos (permisos.prt) desde el Subsistema de Sesiones a la estación donde se ejecuta el Subsistema de Control de Acceso
- Transmitir el archivo de registros fuera de línea desde el computador del Subsistema de Control de Acceso hacia el computador del Subsistema de Sesiones

Protocolo para la transmisión de archivos

Transmisión de archivo fuera de línea (fdl.prt)



Transmisión de archivo de permisos (permisos.prt)



Para este proceso el protocolo es sumamente simple, el componente fuera de línea actúa como cliente del Servidor de Puerta del Subsistema de Sesiones. Cuando se trata de enviar el archivo de registros fuera de línea, envía el requerimiento 2:ENVIAR y a continuación los datos del archivo fdl.prt. Cuando va a recibir el archivo de permisos, envía el requerimiento 3:RECIBIR, y a continuación recibe todos los datos que el servidor le envíe.

3.9. Estructura De Archivos Utilizados

Archivo de Permisos (permisos.prt)

Este archivo es transmitido desde el Servidor de Puerta del Subsistema de Sesiones para que en caso de un problema en la red el subsistema de control de acceso pueda trabajar. Este archivo es de tipo texto y contiene la siguiente información.

- Identificación de estudiante
- Código de usuario (en sistema Unix)
- Nombre del estudiante
- Grupo
- Horas asignadas en el periodo
- Minutos asignados diarios
- Minutos utilizados en el periodo
- Minutos utilizados en el día

Archivo de Fuera de línea (fdl.prt)

Este archivo es generado por el Subsistema de Control de Acceso cuando se encuentra funcionando sin conexión a la red. Una vez que la red se recupera, el archivo es transmitido hacia el Servidor de Puerta del Subsistema de Sesiones para que sea procesado. Este archivo al igual que el anterior es de tipo texto y contiene los siguientes datos.

- Código del usuario en sistema Unix
- Identificación del estudiante
- Fecha de ingreso
- Hora de ingreso

Archivo de Parámetros (portero.ini)

Adicionalmente el subsistema utiliza un archivo local de parámetros internos para la aplicación, este archivo es un archivo de inicialización de Windows (.ini) que contiene las siguientes secciones y entradas :

[PORTERO]

IpAddrDestinoClientePortero = Dirección IP del Servidor de Puerta

PuertoDestinoClientePortero = Puerto del Servidor de Puerta

PuertoServidorPortero = Puerto utilizado por el componente servidor de control de puerta

WinsockIni= Path del archivo de inicialización del archivo de inicialización de trumpet

[GENERAL]

TimeOut= Valor de timeout para procesos

SignalTime= Tiempo de duración del pulso enviado al circuito de la puerta

UsarArchivoLocal= Indicador de trabajo fuera de línea

PuertoSerialLectora= Puerto serial para la lectora

PuertoSerialPuerta= Puerto serial para controlar la cerradura

[AUTENTICADOR]

IpAddrDestinoClienteAutenticador=Dirección IP del servidor para autenticación

PuertoDestinoClienteAutenticador=Puerto para servidor de autenticación

3.10. Instalación Y Configuración

Antes de proceder a la instalación del programa propiamente dicho, se deben cumplir algunos requerimientos de instalación de software base en el equipo a utilizarse que se detallan a continuación:

- DOS 3.3 ó superior
- MS Windows 3.1 ó superior
- Driver controlador de la tarjeta de red
- Trumpet 2.0 ó superior

El programa puede ser instalado utilizando el programa de instalación generado por el Setup Wizard de Visual Basic ó manualmente copiando todos los archivos generados.

3.10.1. Instalación Desde El Programa De Setup

Para ejecutar este programa simplemente se debe ejecutar el programa SETUP.EXE. Este instalador copiará todos los archivos necesarios a los directorios correspondientes en el equipo donde se realiza la instalación y adicionalmente crea un grupo de programas y el icono del ejecutable en Windows para que sea arrancado directamente.

3.10.2. Instalación Manual De Los Archivos

- Crear un directorio denominado PORTERO en el disco duro.

- A este directorio copiar el programa PORTERO.EXE
- Copiar los siguientes archivos al directorio \WINDOWS\SYSTEM del disco duro del equipo donde se está realizando la instalación :
 - MSCOMM.VBX
 - THREEED.VBX
 - VBRUN300.DLL
 - DDEML.DLL
 - VER.DLL

IV. MODULO DE TRANSACCIONES

4.1. Funciones del Servidor.

Este servidor maneja las transacciones en el Laboratorio de Computación esto Requirimientos de Ingresos al laboratorio, tiempo restante de un usuario , desconexion automática de un usuario, transmición de archivos

Se utiliza un servidor concurrente orientado a conexión . En el que el proceso servidor maestro no se comunica directamente con el cliente , en vez de esto espera los requerimientos de nuevas conexiones . Una vez que un requerimiento ha llegado se retorna el descriptor de socket que se va a usar en la nueva conexión . El proceso servidor maestro crea un proceso esclavo para manejar la conexión y permite al esclavo operar concurrentemente . El Servidor de Transacciones consta de un proceso maestro y varios o ningún proceso esclavo.

A continuación se muestra la estructura de los servidores: concurrente orientado a conexión, en donde un proceso maestro acepta cada requerimiento de conexión y crea un proceso esclavo para manejarlo.

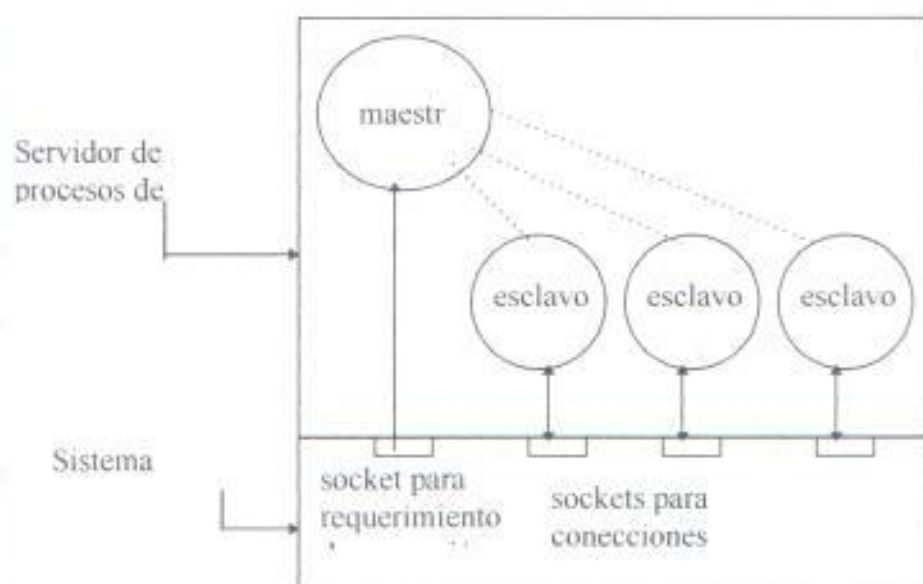


Figura 4.1. Servidor concurrente orientado a Conexión

El Servidor de Transacciones recibe requerimientos de la puerta y del cliente de control de tiempo que tienen 5 mensajes, estos son:

- 1: abrir puerta
- 2: - actualizar ingresos
- 3: envío datos de usuarios
- 4: determina tiempo usuario
- 5: marcar logout a un usuario

Se determina el tipo de requerimiento, y luego llama al script correspondiente que modifica los archivos del sistema.

4.2. Formato Del Mensaje

El formato del paquete que lleva los requerimientos es el siguiente:

comando:parámetro

donde:

comando : es el código designado según sea el requerimiento.

parámetro : es el dato enviado según el comando.

Así tenemos:

1 *abrir puerta* , el código 1 indica un requerimiento de entrada, el cliente de la puerta envía este código al servidor de Transacciones para pedir la verificación del parámetro que envía (que para este caso es el número de tarjeta) como un usuario válido para permitirle el acceso al Laboratorio de Computación.

Cuando el Servidor de Transacciones recibe este requerimiento llama al script *verifica_tarjeta* que se encarga de revisar si ese usuario existe , si está en un grupo activo , si no está sancionado , si tiene tiempo en ese día , y si tiene tiempo disponible en el periodo , si el usuario cumple los requisitos y puede entrar se lo registra en el archivo diario, donde se tienen los siguientes datos:

usuario: el username del usuario

fecha: la fecha en que entro

hora: la hora en que entro

login: hora login , inicialmente coloca 9999 que indica que el usuario

todavía no ha hecho login

logout: hora logout , inicialmente coloca 9999 que indica que el usuario no ha hecho logout.

Maquina: dirección IP o nombre de la máquina , inicialmente coloca 9999 .
La dirección IP de la máquina se actualiza en este archivo cuando el usuario se haga un login exitoso

2 actualizar ingresos , el código 2 le indica al Servidor de Transacciones que se le va a enviar datos de los usuarios que han entrado al Laboratorio de Computación cuando este ha estado fuera de servicio y se registran en el archivo histórico.

3 envío de datos de usuarios , el código 3 es utilizado cuando el cliente de la puerta pide al Servidor de Transacciones los usuarios que tiene acceso al Laboratorio (leídos del archivo usuarios) , para que el cliente de la puerta pueda permitir el paso a los usuarios cuando el Servidor de Transacciones esté fuera de servicio.

4 determina tiempo usuario, el código 4 indica al servidor de accesos que se requiere del tiempo permitido en el día para un usuario determinado en donde el parámetro corresponde al username , para este requerimiento se ejecuta el script tiempo_usuario.

5 logout usuario , el código 5 indica al Servidor de Transacciones que un usuario a sido desconectado manualmente en donde el parámetro corresponde al username de dicho usuario , esto pasa cuando el programa que controla el tiempo en una PC indica

que el tiempo diario de esa persona ha terminado , para esto se ejecuta el script `marca_logout` que lo registra en los archivos `diario` y `conectados`.

4.3. Instalación y Configuración

El archivo fuente del programa para controlar las Transacciones en el Laboratorio se llama `servidor.c` ,el que debe estar guardado en el directorio `$HOME/Proyecto/servidor` , donde se encuentran los archivos ejecutables del sistema.

Para compilar el programa y crear un ejecutable se ejecuta la siguiente línea:

```
comp servidor
```

donde :

`comp` es un archivo batch que contiene las siguientes líneas :

```
gcc -c $1.c
```

```
gcc $1.o -o $1
```

y `servidor` se refiere al nombre del programa `servidor` de Transacciones en el Laboratorio de Computación.

Para levantar el servidor de Transacciones en el puerto por default (1070) se ejecuta la siguiente línea:

```
servidor &
```

Para levantar el servidor de Transacciones en algún puerto específico (por ejemplo el puerto 1170) se ejecuta la siguiente línea:

```
servidor 1170 &
```

Crons del Sistema:

Además se creo un archivo llamado mycron que se encuentra en el directorio \$HOME/Proyecto/datos para la actualización de tiempos utilizados por los usuarios, el contenido de este archivo es el siguiente:

minutos	dia	m	d/m	m/y	Script que se ejecuta
0,5,10,15,20,25,30,35,40,45,50,55	*	*	*	*	\$HOME/Proyecto/shells/logout_auto
0	19	*	*	*	\$HOME/Proyecto/shells/final_dia

en donde:

```
0,5,10,15,20,25,30,35,40,45,50,55      *      *      *      *
```

```
$HOME/Proyecto/shells/logout_auto
```

indica que todos los días cada 5 minutos se ejecute el script logout_auto el que lee cada línea del archivo "conectados" para verificar que no se le ha terminado el tiempo a ningún usuario, si es así se lo elimina de conectados y se ejecutara el script "marca_logout" para poner la hora del logout en diario mientras que el programa de control de tiempo en la máquina cliente lo debe haber desconectado

```
0 19 * * * $HOME/Proyecto/shells/final_dia
```

indica que todos los días a las 19:00 horas se ejecute el script "final_dia" el que revisa el archivo "conectados" para verificar que no hay nadie conectado si es así se ejecutan los scripts "actualiza_tiempos" y "diario_historico", el primero va a la tabla de usuarios en donde se suma el tiempo consumido en el día al tiempo consumido en

periodo y pone en cero el tiempo diario del usuario , el segundo copia todo el archivo diario al histórico

Una vez creado el archivo mycron se tiene que ejecutar la siguiente instrucción:

```
crontab mycron
```

donde:

se somete el archivo mycron al cron del sistema.

4.4. Diseño Del Sistema De Archivos

La estructura de archivos queda ordenada de la siguiente forma:

\$HOME/Proyecto/

/serv_adm

/servidor

/shells

/datos

/logs

/temp

Servidor

Existe un archivo llamado "servidor.h", éste contiene las definiciones, constantes y funciones básicas para construir un programa servidor.

Básicamente existen dos programas servidores: servidor y serv_adm, para requerimientos de acceso al laboratorio, y de administración

respectivamente.

Se utilizan variables de ambiente para los directorios en los cuales se almacenaran archivos, tanto para los programas como para los scripts de shell.

HOME

DIRTEMP=\$HOME/Proyecto/temp

DIRDAT=\$HOME/Proyecto/datos

DIRLOG=\$HOME/Proyecto/logs

DIRSHELL=\$HOME/Proyecto/shells

Shells.-

En este directorio se almacenaran todos los scripts que el sistema emplea.

Datos.-

Los principales archivos de datos a almacenar son:

usuarios.

administradores.

grupos

config

Logs.-

Se mantendran los siguientes archivos:

diario.

Este archivo registra todos los eventos de ingreso al laboratorio y uso de PC sucedidos en el dia.

historico.

Este archivo es idéntico al anterior, y será actualizado al final del día
conectados.

Este archivo ha sido creado por facilidad de operación de programa que controla el
tiempo de uso de la PC.

eventos.

Este archivo es de uso exclusivo del programa de administración

Temp.-

Este directorio tiene los archivos temporales

V. Sistema De Administración (Servidor)

5.1. Función

Este módulo es un programa servidor en ambiente unix , que provee la interface necesaria al cliente administrador para el ingresos y actualización de las cuentas por usuario y por grupo de usuarios así como también provee de cierto número de reportes de gran utilidad para el administrador del laboratorio. Provee opciones extras tales como abrir, bloquear y desbloquear la puerta

5.2. Diseño E Implementaron.

Este servidor tiene las cualidades se ser

- *STATEFULL*
- *CONCURRENTE.*
- *ORIENTADO A CONEXIÓN*

Statefull por que mantiene información de la conexión actual como es el usuario que se encuentra conectado.

Concurrente por que permite atender a varios clientes a mismo tiempo.

Orientado a conexión por que usa el protocolo TCP/IP para la comunicación entre cliente y servidor.

Este servidor es implementado en C para Unix.

Con el propósito de poner práctica los conocimientos de programación en Cliente - Servidor Usando TCP/IP, adquiridos en el presente Tópico. Además de prestar un servicio al laboratorio de COMPUTACION y a los futuros laboratorios que se implemente en la ESPOL en los cuales se ponga en producción este sistema.

5.2.1. Clientes A Los Cuales Brinda Servicio:

- 1.- Programa cliente que da mantenimiento y consulta de los archivos del sistema.
- 2.- Programa cliente-servidor que controla la puerta de ingreso al laboratorio.

5.2.2. Facilidades Proporcionadas En El Programa De Administración

El Programa de Administración cumple los siguientes requerimientos :

- Provee un mecanismo de seguridad y autenticación a nivel de usuarios autorizados para uso del programa.
- Permite las siguientes consultas:
 - Personas que se encuentran en el Laboratorio
 - Personas que están usando PC's
 - Listado de accesos diarios (al laboratorio y usos de PC's), dado el día
 - Número de accesos y tiempo de uso por usuario (total y por intervalo)
 - Eventos acontecidos por fecha, dado un rango de fechas y un administrador.

- Crear/Editar/Eliminar usuarios y sus permisos
- Crear/Editar/Eliminar grupos y sus permisos
- Manejo remoto de la puerta.
- Bloquear y desbloquear la puerta de manera remota.
- Cambiar clave de administrador

5.2.3. Seguridad Y Autenticación

Al momento de iniciar la ejecución del programa (cliente), se le solicitará al usuario que proporcione su *username* y su *password*, para efectos de autenticación. Sólo los usuarios que tengan permisos como ayudantes estarán autorizados para usar el programa.

5.2.4. Mecanismo De Consultas

El cliente administrativo envía requerimientos en un formato de mensaje reconocible por el servidor. Estos requerimientos proporcionan al servidor los parámetros necesarios para que este realice la consulta.

Creación de Usuarios

Los usuarios se crean de la misma manera, proveyendo el cliente al servidor de un mensaje con un formato idéntico al de un registro en el archivo de almacenamiento de datos de usuarios, como restricciones de creación de usuarios no se permiten crearlos con el mismo código de tarjeta o username.

Eliminación de Usuarios

La eliminación de un usuario, necesita de un requerimiento exclusivo para el efecto. Incluye un código que identifica el requerimiento y el *username* ó número de tarjeta.

Cualquier ayudante puede cambiar la información de los usuarios, inclusive la suya misma.

Creación de grupos de usuarios

La creación de grupos nos facilita el manejo de grupos de usuarios de acuerdo a la conveniencia del administrador del laboratorio.

Para mayor flexibilidad, el sistema permite configurar los grupos con cupo por periodo y tiempo de uso diario de una maquina , además nos permite bloquear grupos y permitir grupos que ingresen sin necesidad de una tarjeta.

Apertura, bloque y desbloqueo remotos de la puerta

Para la apertura remota de la puerta el cliente administrador , hará un requerimiento al servidor de administración . Este registrará el evento de abrir la puerta, bloquear o desbloquear incondicionalmente y a su vez enviará al servidor PORTERO un requerimiento para abrirla.

Diagrama del Servidor Administrativo.

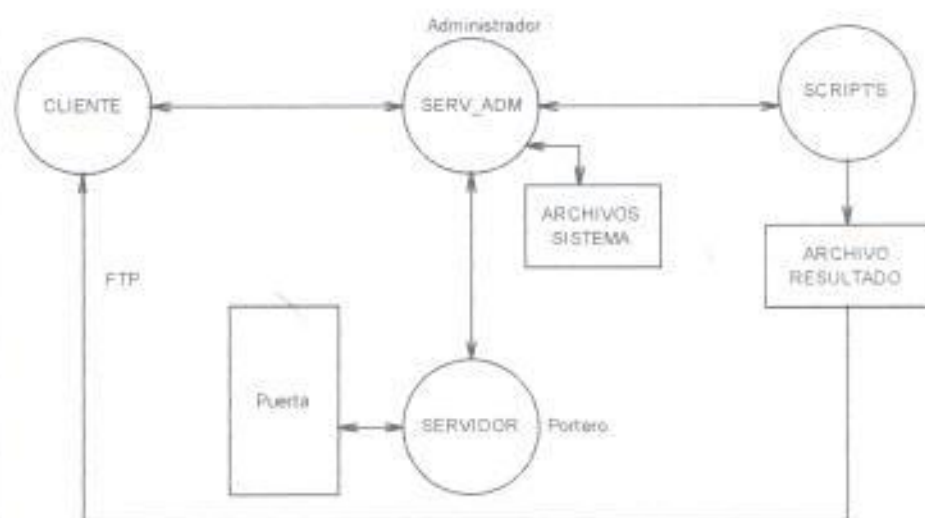


figura 51. Diagrama del Servidor Administrativo.

El cliente administrativo envía un requerimiento al servidor, este filtra el requerimiento y determina si se debe ejecutar un script para proveer la respuesta o si la respuesta se la puede dar de manera directa.

En caso de ser necesario el script a este se le envían los mismos parámetros que se recibe en el requerimiento y el script de acuerdo los parámetros realiza la consulta en los archivos del sistema. Este script puede que genere un archivo de resultado el programa cliente espera por un respuesta afirmativa para proceder a descargar el archivo respuesta.

En caso de no ser necesario un script el mismo programa realiza una actualización o consulta directa de los archivos del sistema.

5.3 Archivos Usados En El Sistema Administrativo.

5.3.1. Introducción

Los Archivos será manejado en modo texto. El delimitador estándar será el carácter ",", por lo que nos permite tener campos de longitud variable.

5.3.2. Archivo Usuarios:

En este archivo están definidos todos los usuarios del laboratorio, además de sus permisos y propiedades.

- Código en la tarjeta.
- Username.
- Apellidos y Nombres. Es una sola cadena (un sólo campo).
- Número de Grupo al que pertenece.
- Cupo por Periodo
- Cupo diario (en minutos).
- Tiempo total utilizado en el día (en minutos).
- Cuenta Bloqueada.

5.3.3. Archivo Grupos

Almacena los grupos de usuarios.

- Código de grupo.
- Nombre de grupo.
- Bloqueado (sí/no).

- Tiempo por periodo(min)
- Tiempo por día(min)
- Permitir ingresar sin marcar tarjeta(si/no)

Los campos de tiempo por periodo o por día sirven como tiempo por omisión en el momento de crear un usuario nuevo y escoger el grupo al cual el pertenece.

3.3.4 Archivo de Administradores

Este archivo almacena los usuarios con su respectiva clave, que son los que tienen permisos para acceder al programa cliente de administración.

- Usuario
- Clave

Por razones de seguridad este archivo se le dará mantenimiento de forma manual, usando alguna herramienta de edición de texto como vi u otro de preferencia del administrador.

5.3.5. Archivo Diario

En este archivo se registrará los accesos al laboratorio en un mismo día.

En el se registra el código universal correspondiente a la tarjeta del usuario en un registro independiente para cada vez que alguien ingresa. Este archivo sólo tiene registrados los accesos del día.

- Usuario
- Fecha (día en que se registra el acceso)
- Hora de ingreso (hora de entrada con la tarjeta).
- Hora login (hora de conexión via nfs).
- Hora logout (hora de desconexión del nfs).
- Hora de entrada (al laboratorio)
- Nombre de Maquina (con la que se conecto a la red)

5.3.6. Archivo Conectados

Mantiene un registro de los usuarios conectados

- Usuario
- Hora Login
- Tiempo restante
- Hora de Entrada (al laboratorio)

- Nombre de maquina (que esta usando en la conexión)

Observaciones:

- Si la HORA DE LOGIN es 9999 , es porque el usuario que entró al laboratorio, no ha echo login todavía
- Ningún usuario puede usar ninguna máquina (por lo tanto no puede hacer LOGIN) si no tiene una registro en el archivo diario.
- Los accesos al laboratorio correspondientes a días pasados son almacenados en el archivo Historia. Este archivo es actualizado diariamente (al final del día por un *cron* de UNIX.

5.3.7. Archivo Histórico.

Tiene la misma función del archivo diario, sólo que a nivel de historia. Su finalidad es la de llevar información de los accesos de días pasados.

- Usuario
- Fecha (día en que se registra el acceso)
- Hora de ingreso (hora de entrada con la tarjeta).
- Hora login (hora de conexión via nfs).
- Hora logout (hora de desconexión del nfs).
- Hora de entrada (al laboratorio)
- Nombre de Maquina (con la que se conecto a la red)

Se actualizará el archivo al final de cada día de manera automática por medio de un *cron* de UNIX.

5.3.8. Archivo Eventos:

1.- Registra las actualizaciones hechas a los archivos

- Usuarios
- Grupos

2.- Los intentos exitosos de :

- Abrir la puerta,
- Bloquear la puerta,
- Desbloquear la puerta.

Campos:

- Username (del administrador)
- Fecha del evento
- Código de operación (cambiar cupo máximo , cambiar cupo diario, bloquear)
- Valor: username o nombre del grupo cuyos permisos se modificaron

Observaciones:

- En el caso de abrir, bloquear y desbloquear la puerta, el campo valor queda vacío.

5.3.9. Archivo Config

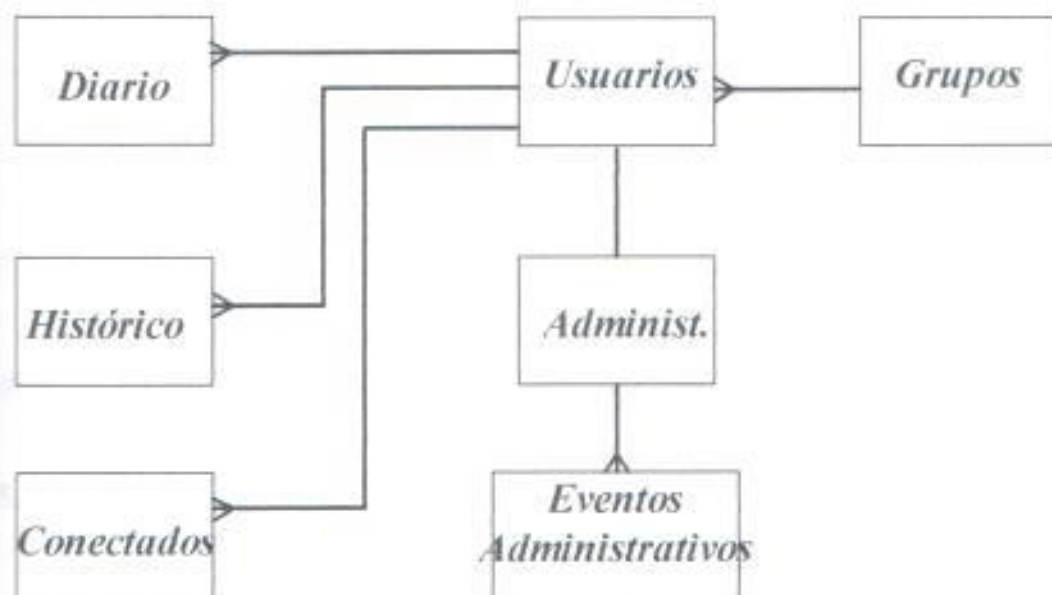
Este archivo mantiene datos de la maquina que tiene el programa que controla el ingreso por la puerta:

- Dirección IP.
- Puerto.
- String de control.

Observaciones

- El string de control es que campo que se actualiza cada vez que se afirma el cliente en el servidor administrativo.

5.3.10. Relación Entre Los Archivos



5.4 Formato De Mensajes

Son requerimientos en formato texto separados por el simbolo ":"

Como cabecera del mensaje se utiliza un nemonico que simboliza la acción a realizar , como argumento se añade los parámetros necesarios para ejecutar la acción requerida:

Eje:

AUTH:alex:more

Nemonico: AUTH

Parámetros: usuario : clave.

Acción a realizar : Autenticar el usuario a utilizar la aplicación servidora.

Separador : los dos puntos .

5.4.1 Mensajes De Ingreso , Consulta Y Modificación De Archivos

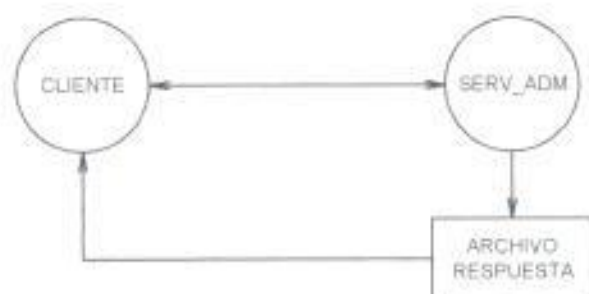


figura 5.2. Comunicación entre cliente Administrativo y Servidor Administrativo

5.4.1.1 Proceso De Autenticación .-

El Cliente antes de poder realizar alguna consulta debe afirmarse en el servidor de administración para lo cual usa el comando

AUTH:username:password.

Este requerimiento es leído por el servidor y procesado buscando en el archivo de administradores si este username y password existes, si es así el devuelve una respuesta de AUTHOK o de lo contrario devuelve un respuesta de AUTHFAIL. En caso de una respuesta afirmativa el cliente esta permitido a realizar cualquier clase de modificación en los archivos del sistema o realizar las consultas proporcionadas por el servidor.

5.4.1.2 Proceso De Ingreso , Consulta Y Modificación De Archivos Del Sistema.

Luego de que el cliente administrativo se halla afirmado en el servidor se tiene varios mensajes "que a continuación detallamos", que podrían ser enviados dependiendo de la consulta que desee. Este mensaje es descodificado y dependiendo del mensaje se ejecuta un script específico , luego de la ejecución del script este da una respuesta de OK o FAIL y genera un archivo en el caso de que el mensajes enviado al servidor sea consulta .

Dependiendo del mensaje que se envió y la respuesta , el cliente sabe si se debe via FTP "bajar" un archivo que es generado por el script que se ejecutó en el servidor.

A continuación detallamos los mensajes , su descripción ,el shell que se ejecuta , las posibles respuestas y el archivo de resultado en caso de un mensaje de consulta.

Tabla #1

<i>Nenomico</i>	<i>Acción a realizar</i>	<i>Shells a ejecutarse</i>	<i>Respuesta</i>	<i>Archivo Generado</i>
AUTH	Autenticación	ladiarios	LOGINOK	
			LOGINFAIL	
LDA	Ingresos por fecha	lacxfecha	LDAOK	lacxfecha.txt
			LDAFAIL	
AN	Tiempo y accesos	lausuarios	ANOK	lausuarios.txt
			ANFAIL	
LOG	Eventos por fecha	levxfecha	LOGOK	levxfecha.txt
			LOGFAIL	
CU	Crear Usuario	cusuario	CUOK	
			CUFAIL	
EU	Modificar Usuario	eusuario,cusuario	EUOK	
			EUFAIL	
DU	Eliminar Usuario	eusuario	DUOK	
			DUFAIL	
LUD	Cargar Usuario	lusuario	LUD	lausuario.tmp
			LUDFAIL	
XU	Buscar usuario	usexiste	XUOK	
			XUFAIL	
CG	Crear grupo	cgrupos	CGOK	

			CGFAIL	
EG	Modificar Grupo	egrupos	EGOK	
			EGFAIL	
DG	Eliminar Grupo	egrupos	DGOK	
			DGFAIL	
LGD	Cargar Grupo	lgrupos	LGDOK	
			LGDFAL	
XG	Buscar Grupo	gexiste	XGOK	
			XGFAIL	
CA	Crear Administrador	cadministrador	CAOK	
			CAFAIL	
EA	Modificar Administrador	eadministrador cadministrador	EAOK	
			EAFAIL	
DA	Eliminar Administrador	eadministrador	DAOK	
			DAFAIL	
LAD	Cargar Administrador	ladministrador	LADOK	
			LADFAIL	
LOGOUT	Desconectar Usuario	marca_logout	LOGOUTOK	

			LOGOUTFAI L	
BU	Buscar Usuarios	busuarios	BUOK	
			BUFAIL	
LDH	Ingresos de hoy	lacxfecha	LDHOK	lacxfecha.txt
			LDHFAIL	
LDM	Maquinas y Usuarios por fecha	laxmxfecha	LDMOK	laxmxfecha.txt
			LDMFAIL	
PIL	Personas dentro del laboratorio	lacxfeca	PILOK	lacxfecha.txt
CLOSE	Desconectarse			

5.4.1.3. Mensajes De Control De La Puerta.

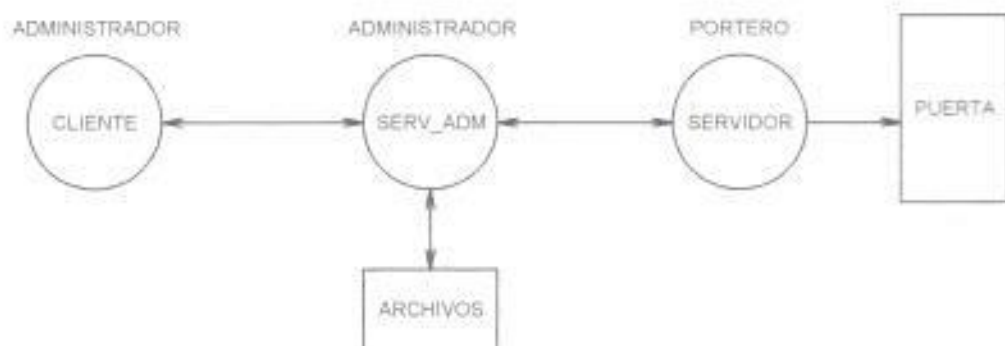


figura 5.3 Comunicación para autorización con ingreso por puerta

5.4.1.4 Autenticación

Al igual que entre el cliente administrativo y el servidor, el servidor Portero tiene que afirmarse en el servidor de administración. Para esto se implemento el siguiente esquema:

El Servidor de la puerta envia un mensaje de autenticación de cliente en el formato:

```
AUTH:username:password
```

El servidor de administración verifica que el usuario y password existan si es asi devuelve un OK caso contrario un FAIL.

En caso de OK el servidor portero genera un string de transacción que lo envía al servidor administrativo con el siguiente formato :

PUERTA:string_transaccioon

El servidor administrativo guarda este string de transacción en el archivo *config* para ser usado cuando el cliente administración requiera abrir , bloquear o desbloquear la puerta. Esto permite que ningún otro programa pueda enviar los mensajes de manipulación de la puerta al cliente portero ya que este verifica que el mensaje que recibe tenga añadido el string de transacción.

Proceso de Manejo de la Puerta:

El cliente Administrador envía el mensaje de Abrir , Bloquear o Desbloquear la puerta EJ.:

OPENDOOR (abrir la puerta)

El servidor administrador recibe este mensaje , establece una conexión con el servidor portero , enviándole el requerimiento mas el strig de transacción Ej.:

OPENDOOR:*string_transaccion*

El servidor administrativo espera por una respuesta del servidor portero , si recibe respuesta el servidor administrativo almacena el archivo de *eventos* lo a ocurrido y pasa el mensaje recibido al cliente administrador.

A continuación los mensajes , descripción , shells que se ejecutan y las posibles respuesta.

Tabla # 2.

<i>Nenomico</i>	<i>Acción a realizar</i>	<i>Shells a ejecutarse</i>	<i>Respuesta</i>
AUTH	Autenticación	lapidarios	LOGINOK
			LOGINFAIL
PUERTA	Setear Password de la puerta	chgpwd	PUERTAOK
			PUERTAFAIL
LOCKDOOR	Bloquear la puerta	regeventos	LOCKDOOROK
			LOCKDOORFAIL
UNLOCKDOOR	Desbloquear puerta	regeventos	UNLOCKDOOR OK
			UNLOCKDOOR FAIL
OPENDOOR	Abrir la puerta	regeventos	OPENDOOROK
			OPENDOORFAIL
CLOSE	Desconectase		

5.5. Compilación , Instalación Y Configuración

El archivo fuente del programa servidor de administración, se llama `serv_adm.c`, el que debe estar en el directorio `$HOME/Proyecto/serv_adm/`, donde se encuentran los archivos fuentes de este servidor del sistema.

Archivos Fuentes:

`serv_adm.c`: Programa Principal
`serv_fun.h`: Funcioines del Programa Administrador
`servidor.h`: Funciones de Comunicación con Socket (TCP/IP)

Compilar el programa fuente.

Para compilar el programa y crear un ejecutable se ejecuta la siguiente línea:

```
comp serv_adm
```

donde :

comp es un archivo batch que contiene las siguientes líneas :

```
gcc -c $1.c
```

```
gcc $1.o -o $1
```

y *serv_adm* se refiere al nombre del programa servidor de Administración

Levantar el servidor de administración

Para levantar el servidor de Administración en el puerto por default (7020)

- Posicionarse en el directorio donde se encuentre el ejecutable `serv_adm`

debe ser: \$HOME/Proyecto/serv_adm/

- Digite la siguiente línea de comando.

```
serv_adm & (lo pone a ejecutarse en background)
```

Para levantar el servidor de administración en algún puerto específico (por ejemplo el puerto 7021) se ejecuta la siguiente línea:

```
serv_adm 7021 &
```

Crear archivos en el servidor Unix.

Crear el Archivo vacío de usuarios, eventos, diario, conectados en los respectivos directorios.

```
/SHOME/Proyecto/datos/usuarios
```

```
/SHOME/Proyecto/log/diario
```

```
/SHOME/Proyecto/log/conectados
```

```
/SHOME/Proyecto/log/eventos
```

- Crear Archivo de grupos con grupos por default como administradores y ayudantes.

Nombre: /SHOME/Proyecto/datos/grupos

Formato:codigo.Nombre:Bloqueo:tiempo_periodo:tiempo_diario:lng_sin_Tg:

Ejemplo:

```
0:Administradores:no:1000:10:si
```

```
1:Ayudantes:no:1000:10:si
```

- Crear archivo de Administradores

Nombre : /\$HOME/Proyecto/datos/administradores

Datos:

Formato: usuario:clave

Ejemplo:

Alex:Moreno

Jessica:Malta

- Crear Archivo de configuración del cliente en la puerta

Nombre: /\$HOME/Proyecto/datos/config

Formato : Dirección IP:Puerto

Dirección I/P : Es la dirección IP de la maquina donde se encuentra el programa cliente que controla la puerta de ingreso al laboratorio .

Puerto: Es un puerto disponible en la misma maquina .

Ejemplo:

192.188.34.2:2001.

VI. Servidor PCNFSD

6.1. Función.-

El demonio pcnfsd provee los siguientes servicios:

- **Autenticación** :- Una forma para que los usuarios se identifique a la red y garantizar apropiados privilegios para acceso a los archivos y ejecución de los programas.
- **Servicio de acceso para la cola de impresión** :- Provee a los usuarios de PC una forma de imprimir en impresora conectada al servidor en la red.

6.1.1. Autenticación y Seguridades del Sistema

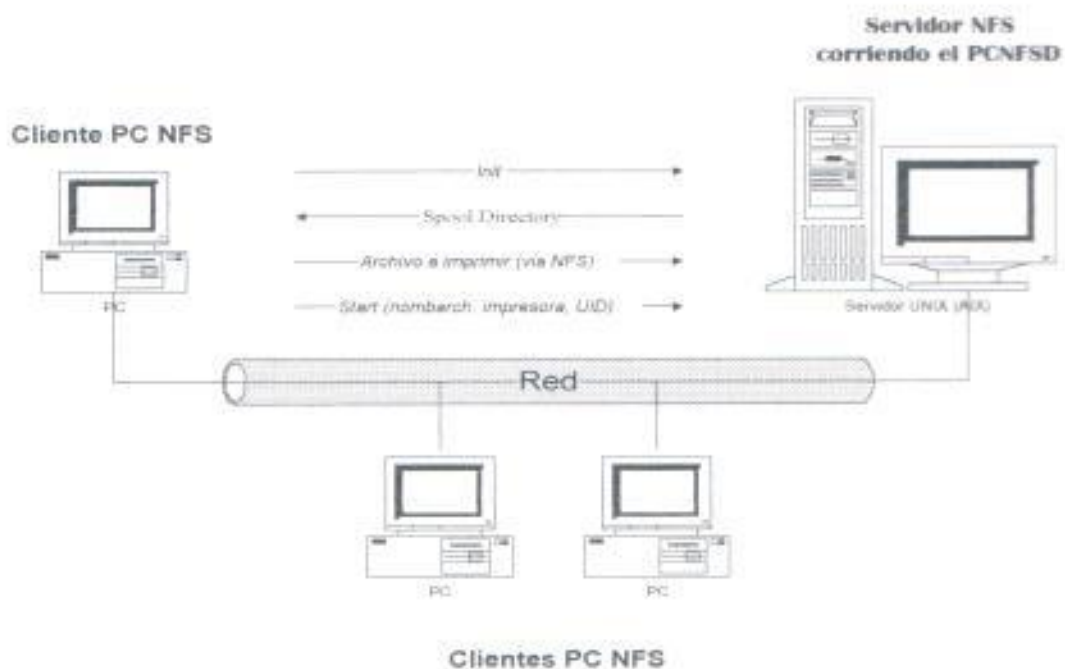


Figura 6.1. Funcionamiento Normal de una Red PCNFS con todos sus servicios

El programa de login toma el username y password, ambos encriptados, y llama al procedimiento de autenticación en el `rpc.pcnfsd` en el sistema que es actualmente el servidor de autenticación. Este procedimiento si es exitoso retorna un user ID y un

grupo ID(GID) para ser usado cuando construya las credenciales para el usuario, o este falla, indicando que el nombre y password es inaceptable. Estas credenciales son usadas para el subsecuente acceso a archivos NFS.

Si el servidor de autenticación esta corriendo el demonio `rpc.pcnfsd` versión 2, este también retorna el grupo secundario, el `umask`, y la información del directorio `home` (tales como el nombre del servidor y el nombre del camino del directorio `home`).

Un usuario que no se logonee dentro de la red es asignado el `username default`, `nobody` (UID -2, GID -2). Cuando el usuario ejecuta la tarea bajo el `username nobody`, Todos los archivos que ellos crean son propiedad del `nobody`. En estas situaciones el sistema de manejo de cuentas y administración no son posible.

Se debe conocer además que el PCNFS no es más seguro que el sistema UNIX el cual no autentica usuarios sobre una red. Por ejemplo, PCNFS usa una minimal encriptación para chequeo de password. Este chequeo es realizado para determinar los usuarios quienes están casualmente analizando el tráfico de la red, más que como una defensa en contra de un ataque criptográfico.

6.1.2. Soporte para compartir impresora

El programa `rpc.pcnfsd` version 1 habilita al usuario hacer uso básico de los servicios de impresión.

La impresión básica significa que un usuario tiene que habilitar a conectar una impresora de red e iniciar un trabajo de impresión. Además para este servicio, `rpc.pcnfsd` versión 2 provee al usuario con los siguientes refuerzos en el servicio en la impresión:

- Buscar por una impresora en la red
- Ver la cola de impresión en la red
- Cancelar o remover trabajos de impresión en la cola de impresión de la red.

6.1.3. Determinando Versión de `rpc.pcnfsd`.

Hay 2 versiones de el programa `rpc.pcnfsd`:

- **Versión 1 de el `rpc.pcnfsd`** - El demonio del `rpc.pcnfsd` versión 1 provee al usuario autenticación y servicios básicos de impresión.
- **Versión 2 de el `rpc.pcnfsd`** - El demonio del `rpc.pcnfsd` versión 2 provee añadiduras para la autenticación del usuario y refuerzos básicos para el servicio de impresión. Mientras estos servicios de implementaciones adicionales son de uso general, el servicio de impresión ha sido provisto para ser compatible con Microsoft Windows 3.1 y Windows for Workgroups 3.11.

El servidor `rpc.pcnfsd` soporta ambas versiones de el protocolo `pcnfsd`.

6.1.4. El log `wtmp`

Usted puede usar el mecanismo de logging del `wtmp` de Unix dentro del PCNFS. Cuando el registro `wtmp` esta habilitado, el demonio `rpc.pcnfsd` añade un registro a la base de datos del `wtmp` para cada acceso desde una PC.

Si Ud. no esta seguro si su demonio `rpc.pcnfsd` usa `wtm`, usted puede usar el comando `last`. Este comando busca en la base de datos todos los logins y logouts registrados. Si entrada al sistema en este archivo tiene la cadena `PC-NFS` en la segunda columna, entonces `rpc.pcnfsd` esta usando el `wtmp`. Alternativamente, usted puede revisar el archivo `common.h` o el archivo `makefile` en el `rpc.pcnfsd` en el `rpc.pcnfsd` edificado en `c` directorio para ver si contiene la opción `wtmp`.

6.1.5. Llevando `rpc.pcnfsd` a otros servidores NFS.

NFS esta disponible en muchas diferentes plataformas. Dependiendo de su particular implementación NFS, el procedimiento que usted utiliza para llevar a un puerto al servidor `rpc.pcnfsd` debe ser diferente.

Antes usted comenzar el demonio en un puerto, debe estar seguro de leer los comentarios en el código fuente y consultar al vendedor de sus sistema operativo para ver si tal puerto ya ha sido ocupado o para obtener instrucciones del puerto.

El programa `rpc.pcnfsd` esta estructurado como un simple servidor RPC, usando los más altos niveles de llamada RPC. Si las librerías para el RPC no es parte de sus librerías standard, usted debe modificar el archivo `makefile` en el directorio conteniendo los archivos de código fuente de el `rpc.pcnfsd` para buscar las apropiadas librerías. Caso contrario si su sistema ya contiene las librerías necesarias para el RPC, el `rpc.pcnfsd` solo necesita recompilarse.

6.2. Procedimiento y Modificaciones realizadas.

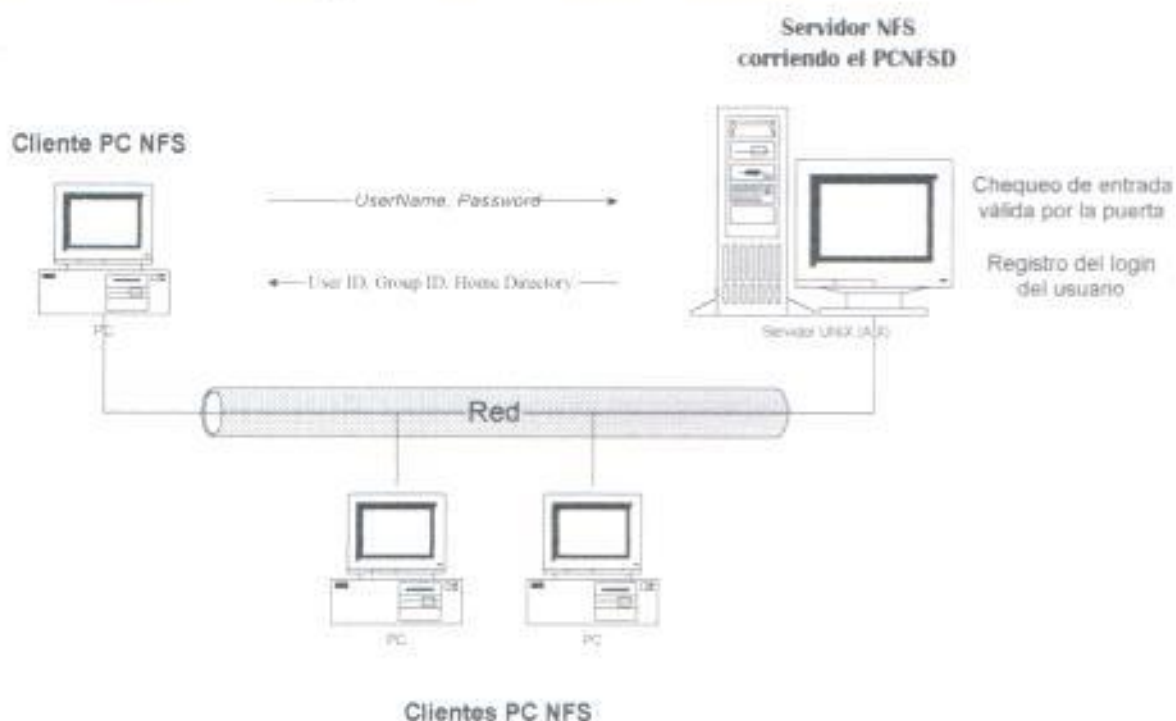


Figura 6.2. Esquema de como el servidor funcionara con las modificaciones

Para el proyecto se configuro la parte de autenticacion. Esta funciona como sigue:

La maquina cliente PCNFS envia el User ID y el password al servidor pcnfsd en una estructura incluida en la llamada a un procedimiento PCNFSD_AUTH. Este revisa si este es valido y si lo es envia una constante de exito (AUTH_RES_OK) y envia una estructura que contiene el UID, GID y el home directory como datos principales. Si no envia una constante de fallo (AUTH_RES_FAIL).

Luego, el cliente PCNFS envia el UID y el GID en los requerimientos al NFS server. El PCNFSD no es necesario para poder usar el NFS. Simplemente suministra un servicio de autenticacion con el fin de controlar el acceso a los archivos. El PCNFSD Y EL NFS no fue hechos como un modelo de seguridad. Incluso el PCNFSD suministra un modelo bastante simple de encriptar el user y password en los

requerimientos de autenticación. Hace una operación XOR con una constante específica y esos resultados son enviados al servidor PCNFSD.

Para resolver el problema de controlar el acceso a una máquina a una persona se hizo ciertos cambios al servidor.

Para que una persona se pueda conectar necesita las siguientes condiciones:

Haya entrado correctamente.

No estar conectado en otra máquina.

Los nuevos controles que se añadieron al PCNFSD fueron

Verificación del archivo de log DIARIO para ver si es válido

Si está correcto marca la hora de login y la máquina cliente en el archivo DIARIO y CONECTADOS

6.3. Manejo de archivo

El programa pcnfsd modificado trabaja con 2 archivos del sistema desarrollado que son diario y conectados.

El procedimiento para las modificaciones del archivo diario es el siguiente:

- 1.- Si un usuario es ingresado correctamente este llama a un procedimiento llamado `actualizar_diario`.

- 2.- El procedimiento actualizar_diario llama al script marca_login el que se encarga de registrar la hora de login del usuario en el archivo diario.
- 3.- El mismo script se encarga de anadir la direccion IP o el nombre del host del cliente en el archivo diario.
- 4.- El script marca_login se encarga de llamar al script anade_conectados que modificara al archivo conectados, cuyas modificaciones se detallan a continuacion.

Nota: Este procedimiento es unicamente valido en caso de que un usuario ya halla ingresado por la puerta. De aqui si un usuario no ha pasado por la puerta con su tarjeta o se halle bloqueado o sancionado, no podra utilizar ninguna PC asi ingrese su User y Password correctamente, ya que no se encuentra registrado dentro del archivo diario, donde el usuario es anadido si pasa por la puerta o si el usuario se encuentra ya conectado en una PC.

EL procedimiento para las modificaciones del archivo conectados es el siguiente:

- 1.- El script marca_login se encarga de llamar al script anade_conectados.
- 2.- El script anade_conectados anade a un usuario en la hora indicada de entrada y de login junto a su tiempo maximo de permiso.

- 3.- Este archivo servira para realizar consultas para conocer facilmente quienes estan conectados en un momento determinado.

6.4. Instalacion y Configuracion

Para la instalacion del programa Pcnfsd se deben seguir los siguientes pasos:

1. Conseguir el codigo fuente del servidor rpc.pcnfsd. El codigo se lo puede obtener de uno de los siguientes lugares:

- <http://nic.zcu.cz/ftp/pub/security/cert/tools/pcnfsd/pcnfsd.93.02.16-cert-dist.tar.Z>
- <ftp://ftp.cert.org/pub/tools/pcnfsd/pcnfsd.93.02.16-cert-dist.tar.Z>
- <ftp://ftp.cert.dfn.de/pub/tools/net/pcnfsd/pcnfsd.93.02.16-cert-dist.tar.Z>

Existen mas sitios donde se los puede encontrar.

2. Usar el comando `uncompress` para desempaquetar el archivo `pcnfsd.93.02.16-cert-dist.tar.Z`

```
uncompress pcnfsd.93.02.16-cert-dist.tar.Z
```

3. Utilizar el comando `tar -xvf` para desempaquetar el codigo fuente:

```
tar -xvf pcnfsd.93.02.16-cert-dist.tar
```

4. Se generara automaticamente un directorio llamado pcnfsd que contedra todos los fuentes del archivo pcnfsd.
5. Realizar los cambios necesarios para que el servidor funcione con los requerimientos que deseamos. En nuestro caso se lo valido para que lea el archivo diario para permitir el acceso de un usuario. Ademas se lo valido para no permitir que un usuario se conecte mas de una vez en una PC.
6. Como los fuentes que se bajaron no tenia un makefile para el aix, se disenio un makefile para poderlo compilar en el servidor AIX.
7. Ubicarse en el directorio donde se encuentra el codigo fuente del pcnfsd y ejecutar lo siguiente:

make aix

Automaticamente se creara un directorio aix donde se ubicara todo los programas en forma objeto ademas del ejecutable rpe pcnfsd.
8. Entrar o conectarse como root.

Por ejemplo

```
fiac > su
```

```
Password: <password>
```

9. Copiar el programa `rpc.pcncsd` al directorio `/usr/sbin`.

```
cp rpc.pcncsd /usr/sbin
```

10. Editar y añadir en el `/etc/inet.d` el programa `rpc.pcncsd` para que se cargue cuando se reinicializa el servidor.

VII. CLIENTE DE CONTROL DE TIEMPO

7.1. Funcion

El Cliente de Control de Tiempo tiene como funcion principal controlar el tiempo de permanencia en una maquina de un usuario, solo cuando este se encuentre en el ambiente windows.

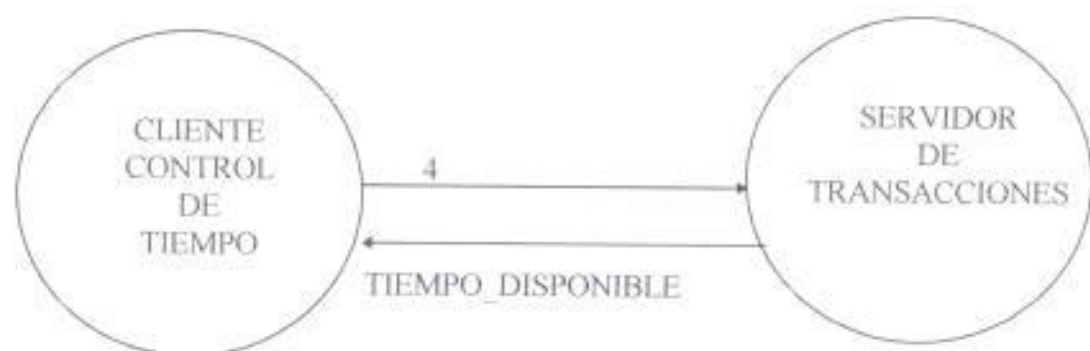


Figura 7.1. Esquema para obtención de Tiempo Disponible

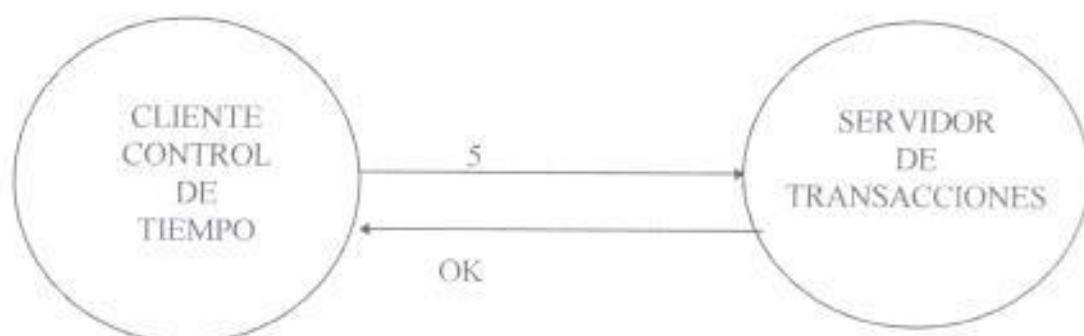


Figura 7.2. Esquema para Indicar a Server Desconexión del Usuario.

El Cliente de Control de Tiempo envia un requerimiento al Servidor de Transacciones pidiendo el tiempo disponible de conexion del usuario que se conecto. Para ello se le envia al servidor el mensaje 4.

El programa obtiene el tiempo disponible de un usuario, y permanecera corriendo durante este tiempo.

El Cliente enviara un mensaje de advertencia al usuario 5 minutos antes de que se termine su tiempo para que grabe y cierre todos los cambios realizados en los documentos o archivos modificados.

Una vez que su tiempo ha terminado el programa envia un mensaje indicando el evento.

Antes de reiniciar el computador, el programa envia al servidor un mensaje de que el usuario ha sido desconectado y con ello el servidor lo elimina del archivo conectados.

El mensaje enviado es el numero 5.

Un usuario tambien puede dar Logout antes de que se le termine el tiempo para ello debe presionar el boton de logout ubicado en el reloj, el sistema no permite salir si previamente no se ha presionado logout. Tambien envia el mensaje 5.

VIII Cliente Administrador

8.1. Función

El programa *Cliente Administrador*, le permitirá al usuario realizar todas las actividades de control de un laboratorio.

Las Actividades de control que el usuario puede realizar son:

- Trabajar con las Consultas
- Trabajar con la Puerta
- Trabajar con los Usuarios
- Trabajar con los Grupos

El programa *Cliente Administrador* hace uso de un archivo de configuración *Admin.ini* que lo podemos editar con el programa *Configuración*.

8.2. Diseño

8.2.1. Programa de Configuración

El programa de configuración permite editar el archivo *Admin.ini* que permite ingresar la información de la máquina donde se está ejecutando el programa *Servidor de administración*; existen dos campos generales de información que se deben ingresar:

1. Información del Servidor de Administración.

Servidor de Administración es un programa que corre en un sistema operativo Unix que se encarga de atender los requerimientos del programa cliente .

El programa cliente Administrador requiere saber dos parámetros principales de la máquina donde está ejecutándose el servidor de administración:

Dirección IP: La dirección IP de la máquina en donde se está corriendo el programa Servidor de Administración.

Puerto: El valor del puerto TCP que está asignado para que atienda los requerimientos del programa Cliente de Administración

2. Información del Servidor FTP

Para transferir archivos el Sistema hace uso de la aplicación FTP por lo que se necesita conocer todos los parámetros para poder establecer una sesión FTP entre el Servidor y Cliente de Administración. Estos parámetros serán descritos a continuación:

Usuario: Es el nombre de un usuario que cumpla con las siguientes condiciones: estar definido en el Servidor Unix , tener permiso de realizar sesiones FTP y que tenga permisos sobre los directorios definidos posteriormente.

Password: Es la clave que le permite el ingreso al usuario definido en el campo anterior.

Directorio Temp: En este campo se debe especificar el directorio en que el Servidor en la máquina Unix guarda los archivos que genera después de ejecutar el requerimiento que el Programa Cliente le haya solicitado. Es en este directorio que el Programa Cliente va a buscar los archivos para copiarlos a su máquina por medio de la aplicación FTP.

Directorio Datos : Este campo deberá contener el directorio en el cual el Servidor Unix guarde los archivos con las tablas que contienen la información referente a usuarios, grupos, permisos, etc.

8.3. Programa Cliente Administrador

El programa cliente administrador exige en su inicio la validación del Administrador, la persona que desee ingresar al sistema deberá tener un Nombre de Usuario y una Clave, si cualquiera de estos dos parámetros son erróneos la aplicación negará el Ingreso a la Aplicación.

La Pantalla de Inicio le permitirá al administrador 3 intentos para el ingreso correcto de los parámetros, una vez expirados estos intentos el modulo de cliente Administrativo se cerrará.

Luego del inicio del programa se muestra una pantalla con todas las opciones que el programa dispone.

A continuación describiremos todas las opciones del cliente administrativo:

8.3.1. Administración: Cambiar Clave

Descripción

Esta opción permitirá al usuario cambiar su clave de ingreso al sistema.

Formato del requerimiento

EA

Formato de la Respuesta

EADK	El cambio de clave fue satisfactorio
EAFAIL	No se pudo realizar el cambio de clave

8.3.2 Consultas del Cliente

El administrador puede realizar consultas sobre el estado del laboratorio. Las consultas que el administrador puede realizar son las siguiente:

- Usuarios Conectados
- Ingresos al Laboratorio del día actual.
- Ingresos al Laboratorio por Fecha
- Ingresos al Laboratorio por Usuario
- Eventos Administrativos
- Accesos por máquina

En todas las consultas el programa Servidor Administrador genera un archivo en formato texto en un directorio temporal, este archivo luego es bajado a través de FTP por el programa cliente. En cada descripción de las consultas se especifica el archivo respuesta generado así como el directorio en la máquina servidora y cliente en donde se encuentra ubicado este archivo; en el servidor el archivo es generado en un directorio que se especifica en el programa configuración al cual llamamos *dir_Temp*; en el cliente el archivo se almacena en un subdirectorio del directorio *dir_app* que es el archivo en donde se encuentra instalada la aplicación.

8.3.3 Consultas: Usuarios conectados

Descripción

Usuarios en el laboratorio es en donde el Administrador va a poder observar el listado de los alumnos a los cuales el Servidor de Puerta les ha permitido el acceso al laboratorio; y que ya se han ingresado su usuario y password en alguna máquina.

El Sistema le dará al administrador el User ID, Nombre, de los usuarios, dirección IP de la máquina, además la Hora de entrada y el tiempo que le queda para poder usar la máquina.

El sistema le da la facilidad al administrador desde esta pantalla de Desconectar manualmente a un usuario si así se lo desea.

Archivo Generado

Servidor administracion	Cliente administración
dir_Temp\ladiarios.txt	dir_app\Temp\ladiarios.txt

Formato del requerimiento

PIL

Formato de la Respuesta

PILOK	Se realizó la consulta y el archivo se pudo generar
PILFAIL	No se pudo generar el archivo

8.3.4 Consultas: Ingresos al laboratorio hoy**Descripción**

Esta consulta le permite al administrador controlar toda las actividades referentes a ingresos al laboratorio del día actual.

El Administrador tendrá un listado de los usuarios con la información de hora en que entró , hora que se registró y a que hora salió del sistema, además del tiempo que lo usó.

Una vez que el listado está en pantalla el administrador podrá clasificar los datos con los siguientes criterios:

Todos: Todos los usuarios

Sin Login : los que aun no se han conectado

Conectados : los que ya están usando una máquina

Desconectados : los que ya se han desconectado

Archivo Generado

Servidor administracion

Cliente administración

dir_Temp/lacxfecha.txt

dir_app\Temp\ lacxfecha.txt

Formato del requerimiento

LDH

Formato de la Respuesta

LDHOK Se realizó la consulta y el archivo se pudo generar

LDHFAIL No se pudo generar el archivo respuesta

8.3.5 Consultas: Ingresos al laboratorio por fecha

Descripción

El administrador podrá preguntar el listado de Accesos por un rango de fecha determinada, escogiendo esta opción el administrador podrá ingresar una fecha inicial y final . El sistema le devolverá un reporte en pantalla con la lista de personas que han ingresado en ese rango de fecha.

El listado contiene el userid, nombre del usuario, nombre de la máquina, hora de login, hora de logout y duración de la sesión.

Archivo Generado

Servidor administracion	Cliente administración
dir_Temp/lacxfecha.txt	dir_app\Temp\ lacxfecha.txt

Formato del requerimiento

LDA:fecha_inicial:fecha_final

Formato de la Respuesta

LDAOK	Se realizó la consulta y el archivo se pudo generar
LDAFAIL	No se pudo generar el archivo

8.3.6 Consultas: Ingresos al laboratorio por usuario

Descripción

Esta opción le va a permitir al administrador conocer, dado el nombre de un usuario, las veces que ha ingresado al laboratorio en un periodo determinado. Este periodo puede ser un rango de fechas que el administrador determine o el periodo total.

El sistema le devolverá al administrador un reporte con la lista de accesos del usuario con la hora que ingresó y la hora que salió durante el periodo que el administrador determine.

Archivo Generado

Servidor administracion	Cliente administración
dir_temp\lausuarios.txt	dir_app\Temp\ lausuarios.txt

Formato del requerimiento

AN:username:fecha_inicial:fecha_final

Formato de la Respuesta

ANOK	Se Realizó la consulta y se pudo generar el archivo
ANFAIL	No se pudo no se pudo generar el archivo de respuesta

8.3.7 Consultas: Eventos Administrativos**Descripción**

Con esta opción el Administrador podrá consultar las actividades que un administrador determinado o todos los administradores hayan ejecutado en un periodo.

El sistema devolverá al administrador un reporte de todos aquellos eventos que el administrador ha realizado, el reporte contendrá el User ID, Nombre, Fecha, Hora, Operación, Parámetro

Archivo Generado

Servidor administracion	Cliente administración
dir_temp\levxfecha.txt	dir_app\Temp\ levxfecha.txt

Formato del requerimiento

LOG:username:fecha_inicial:fecha_final

Formato de la Respuesta

LOGOK	Se realizó la consulta y se pudo generar el archivo
LOGFAIL	No se pudo generar el archivo

8.3.8 Consultas: Accesos por máquinas**Descripción**

El administrador podrá consultar el uso que se ha tenido cada máquina o todas las máquinas; el sistema le permite al administrador realizar la consulta por un rango de fechas:

El sistema le devuelve al administrador un reporte del nombre de la máquina y el nombre del usuario que se registró en esa máquina.

Archivo Generado

Servidor administración	Cliente administración
dir_temp/laxmxfecha.txt	dir_app\Temp\ laxmxfecha.txt

Formato del requerimiento

LDM:máquina:fecha_inicial:fecha_final

Formato de la Respuesta

LDMOK	El cambio de clave fue satisfactorio
LDMFAIL	No se pudo realizar el cambio de clave

8.4. Control de la Puerta

El administrador podrá realizar actividades con la puerta como son: Abrir la puerta, Bloquear la puerta, Desbloquear la puerta.

Además el sistema consta con una barra de herramientas que representa graficamente las diferentes actividades que se realizan con la puerta, los botones se representan a continuación:



A continuación describiremos cada una de las actividades que se realizan con la puerta

8.4.1. Puerta: Abrir la Puerta

Descripción

Esta opción permitirá al usuario abrir la puerta de manera remota.

Formato del requerimiento

OPENDOOR

Formato de la Respuesta

OPENDOOROK	La puerta se pudo abrir
OPENDOORFAIL	La puerta no se pudo abrir

6.4.2 Puerta: Bloquear la Puerta

Descripción

Esta opción permitirá al usuario bloquear la puerta para impedir el acceso de personas.

Formato del requerimiento

LOCKDOOR

Formato de la Respuesta

LOCKDOOROK	La puerta se pudo bloquear
LOCKDOORFAIL	La puerta no se pudo bloquear

8.4.3. Puerta: Desbloquear la Puerta

Descripción

Esta opción permitirá al usuario desbloquear la puerta para habilitar el acceso de personas.

Formato del requerimiento

UNLOCKDOOR

Formato de la Respuesta

UNLOCKDOOROK	La puerta se pudo bloquear
UNLOCKDOORFAIL	La puerta no se pudo bloquear

8.5. Edición, Creación y Eliminación de Usuarios y Grupos

En esta parte del cliente administrativo el administrador podrá realizar actividades relacionados con los usuarios y grupos del sistema. Este menú le permitirá al administrador crear, editar usuarios y grupos.

El subsistema tiene tres opciones:

- Editar Usuario
- Crear Usuario
- Grupos

Las propiedades que debe tener todo usuario para estar definido dentro del sistema son:

Usuario

Es el nombre que el sistema le ha asignado a un Alumno, este valor es único y es la manera en que el sistema reconoce a un alumno.

Tarjeta No

En este campo el administrador verá el número de tarjeta que el usuario tiene, este número es único y está grabado en la tarjeta que cada alumno dispone.

Nombre

En este campo el administrador verá el nombre completo del usuario.

Grupo

En este campo el administrador va a poder a que grupo pertenece el alumno.

Los grupos son asignados por el administrador.

Cupo Diario

Este valor determina la cantidad en minutos que el administrador ha asignado como máximo tiempo diario para que el usuario se le permita acceso al sistema.

Cupo Semestral

Este valor determina la cantidad en minutos que el administrador ha asignado como máximo de uso del sistema en el semestre.

Uso Hoy

Este campo no es editable, le permite al administrador ver la cantidad del tiempo diario que el usuario a estado dentro del Sistema.

Uso Semestral

Este campo no es editable, le permite al administrador ver la cantidad del tiempo durante el semestre que el usuario a estado dentro del Sistema.

Bloqueado

Esta es una propiedad que tienen los usuarios y grupos que le permite al administrador prohibir el acceso a un determinado usuario o grupos de usuarios.

A continuación describiremos cada una de las opciones del subsistema:

8.5.1 Usuarios: Editar Usuario

Cargar datos del usuario

Descripción

Esta opción permitirá al administrador editar todos los campos de información disponibles para un usuario dado. El administrador deberá colocar en el campo usuario el valor correspondiente al username de un alumno con este valor el sistema enviará un requerimiento al servidor solicitándole toda la información disponible de este usuario.

Formato del requerimiento

LUD:username

Formato de la Respuesta

LUD:username:#de_tarj:Nombre:Grupo:Bloq:Cupo_diario:Cupo_Sem:Uso_Hoy:Uso_Sem

8.5.2 Guardar cambios en los datos del usuario

Descripción

Esta opción permitirá al administrador guardar en el servidor todos los cambios que haya realizados en las propiedades del usuario.

Formato del requerimiento

EU:username:#de_tarj.Nombre.Grupo.Bloq.Cupo_diario:Cupo_Sem:Uso_Hoy:Uso_Sem

Formato de la Respuesta

EUOK Se pudo guardar los cambios del usuario en el servidor

EUFAIL No se pudo guardar los cambios del usuario en el servidor

8.5.3 Eliminar usuario

Descripción

Esta opción permitirá al administrador eliminar en el servidor todos los datos que haya de un usuario.

Formato del requerimiento

DU:username

Formato de la Respuesta

DUOK Se pudo borrar al usuario

DUFAIL No se pudo borrar al usuario

8.5.4. Buscar usuario

Descripción

Esta opción permitirá al administrador realizar una búsqueda de un usuario conociendo algún parámetro del mismo. Luego de realizar la búsqueda en el servidor éste genera un archivo que posteriormete es bajado al programa cliente via FTP

Archivo Generado

Servidor administración	Cliente administración
dir_temp\usuarios.txt	dir_app\Temp\usuarios.txt

Formato del requerimiento

XU:parámetro

Formato de la Respuesta

XUOK	La búsqueda fue exitosa
XUFAIL	No se pudo realizar la búsqueda

8.5.5 Usuarios: Nuevo Usuario

Con esta opción el adminsitrador puede añadir usuarios al sistema.

Formato del requerimiento

CU:username:#de_tarj.Nombre.Grupo.Bloq.Cupo_diario:Cupo_Sem::

Formato de la Respuesta

CUOK	La búsqueda fue exitosa
CUFAIL	No se pudo realizar la búsqueda

8.6. Trabajo con Grupos

El manejo de Grupos en el sistema permitirá al administrador crear grupos, borrar grupos y además establecer opciones de bloqueo o desbloqueo de los mismos.

El administrador observará un Lista de Grupos que contiene todos aquellos grupos que están definidos dentro del sistema.

Una vez que el administrador seleccione un grupo el sistema le mostrará las propiedades que tiene dicho grupo las cuales son:

- ID del Grupo
- Nombre del Grupo
- Bloqueado
- Límites de Tiempo Diario y Semestral

A continuación detallaremos las actividades que el administrador puede realizar con los Grupos

8.6.1 Grupos: Nuevo Grupo

Descripción

Con esta opción el administrador puede añadir grupos al sistema

Formato del requerimiento

CG:#del grupo:activo:nombre del grupo:TiempoSemestral:TiempoDiario

Formato de la Respuesta

CGOK	Se pudo crear al grupo
CGFAIL	No se pudo crear el grupo.

8.6.2 Grupos: Guardar Grupo

Descripción

Con esta opción el administrador puede guardar los cambios que ha realizado en las propiedades del grupo.

Formato del requerimiento

EG:#del grupo:activo:nombre del grupo:TiempoSemestral:TiempoDiario

Formato de la Respuesta

EGOK	Se pudo guardar los cambios en el grupo
------	---

EGFAIL No se pudo guardar los cambios en el grupo

8.6.3 Grupos: Eliminar Grupo

Descripción

Con esta opción el administrador puede eliminar un grupo dentro del sistema; para poder eliminar al grupo éste debe de encontrarse vacío es decir ningún usuario deberá pertenecer al grupo.

Formato del requerimiento

DG:#del grupo

Formato de la Respuesta

DGOK

Se pudo borrar el grupo

DGFAIL

No se pudo borrar el grupo

IX. Sistema de Archivos

9.1. Introducción

El Sistema de Archivos será manejado en modo texto. El delimitador estándar será el caracter ":", por ello los campos son de longitud variable.

9.2. Archivo Usuarios:

En este archivo están definidos todos los usuarios del laboratorio, además de sus permisos y propiedades.

- Código universal (de la tarjeta).
- Username.
- Apellidos y Nombres. Es una sola cadena (un sólo campo).
- Número de Grupo al que pertenece (Administrador, Usuario, Mantenimiento , etc.).
- Tiempo maximo del periodo
- Tiempo maximo diario
- Tiempo total utilizado en el periodo
- Tiempo total utilizado en el día.
- Cuenta Bloqueada.

Cada cambio realizado en el archivo Usuarios, debe ser registrado como un Evento en el archivo Eventos.

9.3. Archivo Grupos

Almacena los diferentes grupos de usuarios existentes

- Número de grupo.
- Nombre de grupo.
- Grupo bloqueado.

9.4. Archivo de Administradores

Almacena los administradores existentes en el sistema. Por seguridad para poderlos crear se lo hace de forma manual donde únicamente tiene permiso el root. Los campos que almacena son los siguientes:

Username

Password

Nombre y Apellidos

9.5. Archivo diario

Los accesos al laboratorio en un mismo día, son todos registrados en el archivo diario. En el se registra el código universal correspondiente a la tarjeta del usuario en un registro independiente para cada vez que alguien ingresa. Este archivo sólo tiene registrados los accesos del día.

- Username
- Fecha (día en que se registra el acceso)
- Hora de ingreso (hora de entrada con la tarjeta).

- Hora login (hora de conexión via nfs).
- Hora logout (hora de desconexión del nfs).
- Máquina en la que se conecto

Se creará una fila cuando se REGISTRE CON LA TARJETA llenándose los campos CODIGO, FECHA, y HORA DE INGRESO. Dejándose para pasos posteriores el llenado de los campos restantes.

Observaciones:

- Si la HORA DE LOGIN es cero o nula, es porque el usuario que entró al laboratorio, no ha entrado todavía al sistema.
- Ningún usuario puede usar ninguna máquina (por lo tanto no puede hacer LOGIN) si no tiene una fila en la tabla de accesos.
- Los accesos al laboratorio correspondientes a días pasados son almacenados en el archivo Historia. Este archivo es actualizado diariamente (al final del día por un *cron* de UNIX).

9.6. Archivo Historia.

Tiene la misma función del archivo diario, sólo que a nivel de historia. Su finalidad es la de llevar información de los accesos de días pasados.

- Username.
- Fecha (fecha de ingreso al sistema).
- Hora ingresar (hora de entrada con la tarjeta).
- Hora login (hora de conexión al nfs).
- Hora logout (hora de desconexión del nfs).

Se actualizará el archivo al final de cada día de manera automática por medio de un *cron* de UNIX.

9.7. Archivo Eventos:

Registra las actualizaciones hechas al archivo usuarios.

- Username (del administrador)
- Fecha del evento
- Código de operación (cambiar cupo maximo,cambiar cupo diario,bloquear)

Valor: username o nombre del grupo cuyos permisos se modificaron

Observaciones:

- En el caso de abrir, bloquear y desbloquear la puerta, el campo valor queda vacío.

9.8. Archivo Conectados

Registra los usuarios que se encuentran logoneados en la Pc en un momento determinado.

- Username

- Hora de login
- Tiempo restante de uso
- Hora de entrada al Laboratorio
- Máquina en la que se encuentra conectado

Es utilizado por necesidad de consulta para lograr mayor eficiencia. Sirve para llevar un control de un usuario que se conecta a una PC para llevar el control

9.9.Varios

- En el archivo “/etc/hosts” se creará una fila con la dirección de la “PC que abre la puerta”.
- En un archivo de configuración se actualizarán las siguientes variables de ambiente de UNIX.

CUPO: Para saber cuantas máquinas están disponibles en el laboratorio.

NIVEL: Nivel de seguridad de acceso al Laboratorio, que va de acuerdo al campo “Grupo” de la tabla de usuarios.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Facilidad en las tareas administrativas.
- Se logro un eficiente control de acceso al laboratorio.
- Se optimizó el uso de recursos del Laboratorio.
- Se diseño un sistema de fácil instalación
- Se necesita bajos requerimientos para el desarrollo de el sistema.
- El PCNFS es un servidor que permite compartir recursos.
- Personalizar la sesión de cada usuario.
- Portabilidad del Sistema
- Interface gráfica del Administrador

Recomendaciones

- Crear un Sistema de Archivos.
- Programar las consultas en "C"
- Añadir medidas de seguridad al Sistema
- Generar reportes estadísticos especialmente sobre usuarios, grupos, uso de Pcs, etc.
- Registrar la salida del Laboratorio, posiblemente con otra lectora de tarjeta se puede registrar la hora de salida de una persona del Laboratorio.
- General una Base de Datos Relacional, para agilizar mayores consultas y ayudar tambien a general reportes estadísticos.

APENDICES

A.- MANUAL DEL USUARIO DEL CLIENTE ADMINISTRATIVO.

Manual del Usuario del programa Cliente Administrador

El programa Cliente Administrador le permitirá al ayudante tener el control total del laboratorio en cualquier momento.

Este programa le permitirá al ayudante tener el control sobre tres aspectos:

- Control sobre la puerta, que le va a permitir abrirla, bloquearla o desbloquearla.
- Control sobre los usuarios, permitiéndole añadir, editar o eliminar usuarios.
- Control sobre los grupos, que le permitirá al administrador añadir, editar o eliminar grupos.

Además de estas facilidades que el sistema brinda, también le va a permitir al ayudante realizar una serie de consultas que le van a dar al ayudante una idea clara del estado del laboratorio en cada momento.

El presente documento describe detalladamente cada una de las opciones que el sistema dispone, además de explicar como acceder a cada una de ellas.

Configuración del programa

El programa Administrador Frankie requiere para su ejecución el archivo Admin.ini; existe un programa que se llama Configuración que ayuda al usuario a configurar este archivo; los campos de información que el usuario debe de llenar y su significado se detallan a continuación:

Información de la aplicación servidora Frankie

Servidor Frankie es un programa que corre en un sistema operativo Unix que se encarga de atender los requerimientos del programa cliente.

El programa cliente Administrador requiere saber dos parámetros de principales de la máquina donde está ejecutándose el servidor de administración:

Dirección IP: La dirección IP de la máquina en donde se está corriendo el programa Servidor de Administración.

Puerto: El valor del puerto TCP que está asignado para que atienda los requerimientos del programa Cliente de Administración

Información del servicio FTP

Para transferir archivos el Sistema hace uso de la aplicación FTP por lo que se necesita conocer todos los parámetros para poder establecer una sesión FTP entre el Servidor y Cliente de Administración. Estos parámetros serán descritos a continuación:

Usuario: Es el nombre de un usuario que cumpla con las siguientes condiciones: estar definido en el Servidor Unix, tener permiso de realizar sesiones FTP y que tenga permisos sobre los directorios definidos posteriormente.

Password: Es la clave que le permite el ingreso al usuario definido en el campo anterior.

Directorio Temp: En este campo se debe especificar el directorio en que el Servidor en la máquina Unix guarda los archivos que genera después de ejecutar el requerimiento que el Programa Cliente le haya solicitado. Es en este directorio que el Programa Cliente va a buscar los archivos para copiarlos a su máquina por medio de la aplicación FTP.

Directorio Datos : Este campo deberá contener el directorio en el cual el Servidor Unix guarde los archivos con las tablas que contienen la información referente a usuarios, grupos, permisos, etc.

A continuación se incluye un ejemplo del archivo Admin.ini:

```
[ServidorCentral]
```

```
DirecciónIP=200.9.176.5
```

```
Puerto=7020
```

```
[ServidorFTP]
```

```
Userld=jperez
```

```
Password=Topasoc
```

```
PathGrupos=/home/jperez/Proyecto/datos/
```

```
PathTemp=/home/jperez/Proyecto/temp/
```

Seguridad del Sistema

Para poder ingresar al sistema el usuario deberá tener un usuario Administrador y la clave del mismo. El sistema le permite al usuario cambiar la clave de acceso mediante la opción Cambiar Clave del menú.

El administrador deberá ingresar la clave anterior , ingresar su nueva clave, y por seguridad repetir la clave nueva

Una vez que se hayan ingresado correctamente estos valores el administrador habrá cambiado su clave al precionar el botón aceptar. El administrador deberá recordar esta nueva clave para la siguiente vez que ingrese.

Inicio del Sistema

El programa Cliente Administrador exige en su inicio la validación del Administrador, la persona que desee ingresar al sistema deberá tener un Nombre de Usuario y una Clave, si cualquiera de estos dos parámetros son erróneos la aplicación negará el Ingreso a la Aplicación.

La Pantalla de Inicio le permitirá al administrador 3 intentos para el ingreso correcto de los parámetros, una vez expirados estos intentos la Aplicación Frankie se cerrará.

Consultas

El sistema brinda al administrador la posibilidad de conocer en cualquier momento el estado del laboratorio; para esto el sistema tiene la opción de consultas, las cuales detallamos a continuación:

- Usuarios Conectados
- Ingresos al Laboratorio Hoy

- Ingresos al Laboratorio por fecha
- Ingresos al Laboratorio por Usuario
- Eventos Administrativos
- Accesos por Máquina

Todas estas consultas y sus opciones son detalladas a continuación:

Usuarios Conectados

Usuarios Conectados es en donde el Administrador va a poder observar el listado de los alumnos a los cuales el Servidor de Puerta les ha permitido el acceso al laboratorio; y que ya han ingresado su usuario y password en alguna máquina.

El sistema generará un reporte en pantalla con el listado de las personas que actualmente están usando alguna máquina; el reporte contendrá: el User ID, Nombre, de los usuarios además la Hora de entrada y el tiempo que le queda para poder usar la máquina, además de reportar el nombre de la maquina que está usando.

El sistema le da la facilidad al administrador desde esta pantalla de Desconectar manualmente a un usuario si así se lo desea.

Ingresos al Laboratorio de Hoy

Esta consulta le permite al administrador controlar toda las actividades referentes a ingresos al laboratorio del día actual.

El Administrador tendrá un listado de los usuarios con la información de hora en que entró , hora que se registró y a que hora salió del sistema, además del tiempo que lo usón y la máquina que éste usó.

Una vez que el listado está en pantalla el administrador podrá clasificar los datos con los siguientes criterios:

Todos:

Esta opción es mostrada al principio y contiene el listado completo de los usuarios que han ingresado al laboratorio incluyendo:

Los usuarios que aun no se han registrado en el sistema,

Los usuarios que ya se resistraron y que siguen usando el sistema,

Los usuarios que ya se han desconectados.

Sin Login:

Si el administrador selecciona esta opción va a poder ver aquellos usuarios que han podido ingresar por la puerta pero que aún no se han registrado en el sistema, es decir que no se encuentran usando un PC.

Conectados :

El administrador podrá ver con esta opción aquellos usuarios que ingresaron al Laboratorio y que ya se han registrado en el sistema; es decir aquellos alumnos que están usando las máquinas.

Desconectados:

El administrador podrá ver con esta opción aquellos usuarios que ingresaron al Laboratorio, que ya se han registrado al Sistema y que terminaron de usar la máquina y salieron del sistema.

Ingresos al Laboratorio por fecha

El administrador podrá preguntar el listado de Accesos por una fecha, escogiendo esta opción el administrador deberá ingresar un periodo de tiempo. El sistema devolverá un reporte en pantalla con la lista de personas que han ingresado en este periodo.

El administrador deberá ingresar el periodo de tiempo en base al cual el sistema deberá generar el reporte de ingresos al laboratorio. Para esto el sistema le solicitará que ingrese un rango de fechas:

Fecha Inicial

En este campo el administrador deberá ingresar el valor correspondiente a la fecha de inicio del periodo en que se desea realizar la consulta

El formato de este campo es dd/mm/aaaa.

Fecha Final

En este campo el administrador deberá ingresar el valor correspondiente a la fecha final del periodo en que se desea realizar la consulta

El formato de este campo es dd/mm/aaaa.

Ingresos al Laboratorio por Usuario

Esta opción le va a permitir al administrador conocer, dado el nombre de un usuario, las veces que ha ingresado al laboratorio en un periodo determinado. Este periodo puede ser un rango de fechas que el administrador determine, especificando un intervalo o el periodo total;

Si el administrador elige la opción por intervalo le dice al sistema que va a especificar una periodo de fechas en base a las cuales desea que se haga la consulta

Si el administrador escoje la opción por periodo total especifica que la consulta se haga sin considerar un periodo de fecha. Es decir que considere toda la información que tenga el sistema sin importar la fecha.

El sistema devolverá al administrador un reporte con la lista de accesos del usuario con la hora que ingresó y la hora que salió y la máquina que usó durante el periodo que el administrador determine.

Eventos Administrativos

Con esta opción el Administrador podrá consultar las actividades que un administrador o todos los administradores hayan ejecutado en un periodo dado.

Las opciones de la consulta son:

por administrador

Administrador

Todos

por intervalo

Total

Intervalo

En el primer criterio de consulta el administrador podrá especificar el nombre del administrador cuyas actividades se desee consultar, o seleccionar la opción todos para tener un reporte de las actividades de todos los administradores.

En el segundo de criterio de consulta el administrador podrá especificar un periodo, basado en una fecha inicial y una fecha final, par a la consulta. Nuevamente el adminisitrador podrá seleccionar un periodo total para que la consulta sea hecha sobre toda la información que tenga el sistema sin importa las fechas.

Una vez establecidos los criterios de consultas explicados anteriormente, el sistema devolverá al administrador un reporte de todos aquellos eventos que el administrador ha realizado, el reporte contendrá el User ID, Nombre, Fecha, Hora, Operación, Parámetro.

Accesos por Máquina

Esta consulta le permite al adminstrador conocer las personas que han usado cada una de las máquinas del laboratorio.

El administrador podrá ingresar el nombre de una máquina en especial o hacer una consulta en base a todas la máquinas, también podrá establecer un periodo de tiempo.

Las opciones de la consulta son:

por máquina

Máquina:

Todas

por intervalo

Total

Intervalo

En el primer criterio de consulta el administrador podrá especificar el nombre de la máquina que se desee consultar, o seleccionar la opción todas para tener un reporte de uso de todas las máquinas.

Hay que notar que el nombre de la máquina se refiere a como es reconocida dentro de la red del laboratorio. Este nombre es asignado en el sistema operativo de la máquina, por lo que si se desea cambiar el nombre deberá hacerlo en el Sistema Operativo de la máquina con la autorización del administrador del laboratorio.

En el segundo de criterio de consulta el administrador podrá especificar un periodo, basado en una fecha inicial y una fecha final, para la consulta. Nuevamente el administrador podrá seleccionar un periodo total para que la consulta sea hecha sobre toda la información que tenga el sistema sin importar las fechas.

Trabajar con la Puerta

Entre las funciones que le da el sistema al administrador con el objetivo de que tenga control sobre el laboratorio está el controlar la puerta de acceso al laboratorio para ello tiene tres opciones que puede usar desde la misma aplicación que son:

- Bloquear la puerta
- Desbloquear la puerta
- Abrir la puerta

Es de notar que estas opciones las puede hacer el administrador desde la misma máquina sin necesidad de acercarse a la puerta por ningún motivo.

La explicación de estas opciones se detallan a continuación:

Bloquear la puerta

Con esta opción el administrador podrá Bloquear la puerta en el momento que desee, impidiendo de esta manera el acceso a cualquier alumno que desee ingresar sin importar que tenga tiempo disponible para usar el laboratorio.

El administrador podría usar esta opción si en algún momento se da cuenta que todas las máquinas están siendo usadas, ya que al bloquear la puerta ningún alumno podrá ingresar al laboratorio.

El sistema devolverá al administrador un mensaje comunicándole que la puerta se pudo bloquear, o si existe algún problema en la interconexión de las máquinas del sistema el reporte será que no se pudo bloquear la puerta siendo deber del ayudante revisar la conexión física de las máquinas del Sistema

Desbloquear la puerta

Esta opción le permite al administrador habilitar la puerta para el normal ingreso al laboratorio de los alumnos que estén en capacidad de hacerlo.

Esta opción volverá a activar el Servidor de puerta para que permita el acceso de los usuarios que tienen derecho de usar el laboratorio y prohibir el acceso a aquellos que ya no tienen tiempo o que estén sancionados.

El sistema devolverá al administrador un mensaje comunicándole que la puerta se pudo desbloquear, o si existe algún problema en la interconexión de las máquinas del sistema el reporte será que no se pudo desbloquear la puerta siendo deber del ayudante revisar la conexión física de las máquinas del Sistema

Abrir la puerta

Esta opción le permite al administrador Abrir la puerta de acceso al laboratorio de manera remota.

Esta opción podrá ser usada cuando el administrador desee permitirle el acceso o el egreso a una persona sin que sea registrado por el Servidor de Puerta.

El sistema devolverá al administrador un mensaje comunicándole que la puerta se pudo abrir, o si existe algún problema en la interconexión de las máquinas del sistema el reporte será que no se pudo abrir la puerta siendo deber del ayudante revisar la conexión física de las máquinas del Sistema. Otra razón para que no se pueda abrir la puerta es que la puerta se encuentre bloqueada por el mismo administrador.

Trabajar con los Usuarios

Para poder brindarle al Administrador un control sobre los usuarios el sistema tiene el menú usuarios que le permitirá dos opciones principalmente:

- Editar Permisos de Usuarios
- Nuevo Usuario

El detalle de estas opciones se muestra a continuación.

Editar Permisos de Usuarios

La opción Editar permisos usuarios le permitirá al administrador un control total sobre las propiedades que tiene cada alumno. El Administrador deberá ingresar el nombre del usuario, luego el sistema le mostrará toda la información que tiene sobre este usuario.

El sistema para cada alumno que está definido le asigna propiedades que son información que el administrador puede cambiar si lo desea, las propiedades que definen a un alumno son las siguientes:

Usuario

Tarjeta No

Nombre

Grupo

Cupo Diario

Cupo Semestral

Uso Hoy

Uso Semestral

Bloqueado

La explicación de cada una de estas propiedades se detalla a continuación:

Usuario

Es el nombre que el sistema le ha asignado a un Alumno, este valor es único y es la manera en que el sistema reconoce a un alumno.

Tarjeta No

En este campo el administrador verá el número de tarjeta que el usuario tiene, este número es único y está grabado en la tarjeta que cada alumno dispone.

Nombre

En este campo el administrador verá el nombre completo del usuario.

Grupo

En este campo el administrador va a poder a que grupo pertenece el alumno.

Los grupos son asignados por el administrador.

Cupo Diario

Este valor determina la cantidad en minutos que el administrador ha asignado como máximo tiempo diario para que el usuario se le permita acceso al sistema.

Cupo Semestral

Este valor determina la cantidad en minutos que el administrador ha asignado como máximo de uso del sistema en el semestre.

Uso Hoy

Este campo no es editable, le permite al administrador ver la cantidad del tiempo diario que el usuario a estado dentro del Sistema.

Uso Semestral

Este campo no es editable, le permite al administrador ver la cantidad del tiempo durante el semestre que el usuario a estado dentro del Sistema.

Bloqueado

Esta es una propiedad que tienen los usuarios y grupos que le permite al administrador prohibir el acceso a un determinado usuario o grupos de usuarios.

El administrador podrá ver las propiedades de un usuario y podrá cambiar alguna de ellas si así lo desea, una vez que exista algún cambio el Administrador tendrá que Guardar los cambios para que sea actualizado en el Servidor Administrador.

Búsqueda de un usuario

Si el administrador no recuerda exactamente el nombre del usuario el sistema le da la facilidad de realizar la búsqueda del usuario con cualquier parámetro que el administrador recuerde como puede ser parte del user o del nombre, el número de tarjeta; simplemente el administrador deberá ingresar la cadena de caracteres que recuerde del usuario en el campo usuario y presionar el botón de búsqueda luego el sistema le mostrará un listado completo de los usuarios que en alguna parte de sus propiedades contienen la cadena de caracteres que el administrador ingresó en el campo usuario.

Con esto el administrador selecciona al usuario que el desee y podrá editar todas las propiedades del mismo.

Crear Nuevo Usuario

Con esta opción el administrador habilita a un usuario para que el sistema lo reconozca.

Para que un usuario pueda estar completamente definido el administrador deberá ingresar toda la información que el sistema requiere es decir:

Usuario

Tarjeta No

Nombre

Grupo

Cupo Diario

Cupo Semestral

Uso Hoy

Uso Semestral

Bloqueado

La explicación de estos campos es la misma que la sección anterior.

Cuando el administrador haya ingresado toda la información deberá presionar el botón guardar para que el usuario sea habilitado de trabajar en el sistema.

Trabajar con los grupos

Para permitirle al administrador control total del laboratorio el sistema le da la opción de controlar los grupos que existen de alumnos para ello el sistema incluye el menú Grupos.

La Opción Grupos del sistema le permitirá al administrador crear grupos, borrar grupos y además establecer opciones de bloqueo o desbloqueo de los mismos.

El administrador observará un Lista de Grupos que contiene todos aquellos grupos que están definidos dentro del sistema

Una vez que el administrador seleccione un grupo, en el cuadro lista de Grupos, el sistema le mostrará las propiedades que tiene dicho grupo las cuales son:

ID del Grupo

Nombre del Grupo

Bloqueado

Límites de Tiempo:

Diario

Semestral

La descripción de estos campos se detalla a continuación:

Nombre del Grupo

Este es el nombre que el administrador ha definido para identificar al Grupo.

Límite de Tiempo Diario

Este es un valor en minutos que el administrador le puede asignar por defecto a todo un grupo, que representa la cantidad de tiempo que el alumno puede usar el laboratorio cada día.

Límite de Tiempo Semestral

Este es un valor en minutos que el administrador le puede asignar por defecto a todo un grupo que representa la cantidad de tiempo que el alumno puede usar el laboratorio durante el semestre.

Bloqueado

Esta propiedad le permite al administrador bloquear de manera general a un grupo de usuarios, al estar seleccionada esta opción todos aquellos alumnos que pertenezcan al grupo se les prohíbe el acceso al laboratorio.

Eliminar Grupo

Cuando un grupo está seleccionado el administrador podrá Borrarlo si lo desea, para que un grupo se pueda eliminar, este grupo deberá de estar vacío es decir ningún alumno deberá pertenecer a este grupo.

Nuevo Grupo

Para crear un nuevo grupo el administrador deberá presionar el botón nuevo grupo, con lo que el sistema le mostrará un mensaje solicitándole que ingrese el nombre del nuevo Grupo, si este nombre no existe el grupo será creado, caso contrario el sistema le mostrará un mensaje comunicándole que el nombre del grupo ya existe.

Barra de Herramientas






Además de todas las facilidades que el sistema brinda, el programa cliente administrador cuenta con una Barra de Herramientas que facilita el acceso a las diferentes utilidades del sistema; la barra de herramientas que se muestra la podemos ver a continuación:



Con estos botones el administrador puede tener un acceso inmediato a las principales opciones que el sistema tiene.

La descripción de cada botón y su función se detalla a continuación:

BOTON	NOMBRE	FUNCION
-------	--------	---------

	<i>Abrir la Puerta</i>	Apertura de puerta de manera remota
	<i>Bloquear la Puerta</i>	Bloqueo de puerta de manera remota
	<i>Desbloquear la Puerta</i>	Desbloqueo de puerta de manera remota
	<i>Usuarios</i>	Abre el menú de Usuarios
	<i>Grupos</i>	Abre el menú de Grupos

BIBLIOGRAFIA

1. MARCHUK MICHAEL- QUE BUILDING INTERNET APPLICATIONS WITH VISUAL BASIC.
2. COMER DOUGLAS / STEVENS DAVID Internetworking with TCP/IP VOLUME III
3. MANUAL DEL USUARIO DE PCNFS PRO (SOLARNET)
4. MANUAL DEL USUARIO DE VISUAL BASIC.
5. GROSSMANN UNIX FOR PROGRAMMING
6. MANUALES DEL TRUMPET.
7. DOCUMENTACION SOBRE WINSOCK
8. REFERENCIAS ENCONTRADAS EN INTERNET.