

Ref.: ADV_NK0002
V1.0
ES

NeoLock

MANUAL DE OPERACIÓN DEL SOFTWARE



Marcas

MS-DOS y Windows son marcas registradas de Microsoft Corporation. Todos los otros productos son marcas registradas de sus respectivos dueños.

Advertencia

La información contenida en este documento, puede ser modificada por ADV Technology S.R.L. sin ningún previo aviso. Ninguna parte de este documento se puede fotocopiar, reproducir o traducir a otro lenguaje, sin previa autorización escrita de ADV Technology S.R.L..

Última modificación: 12.11.2001 (dd.mm.yyyy)
Impreso en octubre de 2001

ADV Technology S.R.L.

Vuelta de Obligado 1275 5°B
Capital Federal (C1426BEC)
Buenos Aires – Argentina

www.advtechnology.com.ar

Contenido

Contenido	3
1. Convenciones	7
2. Introducción	8
2.1. Descripción general	8
2.2. Estructura	9
2.2.1. Versión monousuario	11
2.2.2. Versión multiusuario	11
2.3. Gestores de bases de datos	13
2.4. Módulos adicionales y capacidad de expansión	13
2.4.1. Módulo de Visitas	14
2.4.2. Módulo de Personal	14
2.4.3. IOServer	15
2.4.4. Desarrollos a medida	15
2.5. Requerimientos del sistema	16
3. Instalación	17
3.1. El paquete NeoLock	17
3.2. Conexión de la llave de protección	17
3.3. Programas instaladores	18
3.4. Instalación del gestor de base de datos BDE	22
3.5. Instalación del sistema NeoLock	25

3.5.1. Instalación básica	25
3.5.2. Sistemas monousuario	26
3.5.3. Sistemas multiusuario	27
3.6. Instalación de módulos adicionales	27
3.7. Sistemas con otros gestores de base de datos	28
4. Funcionamiento y estructura básicos	29
4.1. Inicio de la aplicación	29
4.1.1. Cómo ingresar al sistema por primera vez	29
4.2. Configuración del sistema	30
4.3. Estructura y configuración del hardware	31
4.3.1. Puertos	32
4.3.1.1. RS-232/RS-485	33
4.3.1.2. Módem	34
4.3.1.3. MDLC Gateway	35
4.3.1.4. TCP-IP	36
4.3.2. Paneles controladores	37
4.3.3. Puertas	42
4.3.4. Alarmas de puerta	47
4.3.5. Alarmas generales	51
4.4. Departamentos	53
4.5. Categorías Vehículos y Usuarios	55

4.5.1. Categorías	55
4.5.2. Usuarios	56
4.5.3. Vehículos	60
4.6. Permisos de acceso	62
4.6.1. Bandas y Horarios	62
4.6.2. Asignación de permisos de acceso	64
4.7. Monitoreo	66
4.7.1. Eventos On-Line	66
4.7.2. Identificación visual	67
4.8. Comandos On-Line	67
4.8.1. Reconfiguración de los paneles	68
4.8.2. Reprogramación de los relojes de los paneles	68
4.8.3. Comandos de puertas y alarmas	69
4.8.4. Comandos de alarmas generales	70
5. Funciones avanzadas	71
5.1. Cámaras digitales asociadas a las puertas	71
5.2. Búsqueda de personas en el área protegida	73
5.3. Desencadenadores y antipassback	74
6. Gestor de reportes	76
6.1. Funcionamiento general de los reportes	76
6.2. Reporte de eventos	77

6.3. Reporte de usuarios	79
6.4. Reporte de permisos de acceso	80
6.5. Reporte de credenciales poco usadas	80
6.6. Reporte de puertas	81
6.7. Reporte de vehículos	81
Apéndice A. Soporte técnico	82
A.1. Reemplazo de componentes	82
A.2. Solución de problemas y Manual para Instaladores	83
Apéndice B. Garantía	84
B.1. Garantía del software	84
Notas	86

1. Convenciones

A lo largo de este documento se utilizarán las siguientes convenciones para diferenciar el significado del texto:

<Teclas> El texto escrito entre los signos <> identifica combinaciones de teclas para realizar acciones en el programa.

Ejemplo:
<Ctrl + S>

Controles Las palabras escritas en negritas en medio del texto identifican controles de la aplicación (botones, menús, etc.).

Ejemplo:
El botón **Modificar** permite...

Menú:Submenú Los menús y sus submenús se escriben en negritas y se separan con dos puntos

Ejemplo:
Comandos.PuertasNormalizar todas

2. Introducción

2.1. Descripción general

El sistema NeoLock permite integrar el control de accesos, la captura de video digital, el control de visitas y el procesamiento de los horarios del personal en un amigable entorno multimedial.

Su arquitectura consiste básicamente en una red de controladores autónomos distribuidos y en una o varias computadoras, mediante las cuales se accede a los datos y se configuran el sistema y los paneles controladores. Éstos últimos pueden funcionar incluso en situaciones donde no están continuamente conectados al resto del sistema. De esta forma se evita que eventualidades tales como fallas en la red de comunicaciones causen la salida de servicio del sistema.

A continuación se listan algunas de las características más importantes del NeoLock:

- Entorno gráfico de uso sencillo.
- Comunicaciones en tiempo real.
- Monitoreo On-Line, que le brinda información acerca de lo que está ocurriendo en las áreas protegidas.
- Panel de comandos On-Line, que le permiten abrir o cerrar puertas, activar o apagar alarmas, etc. desde la/las computadora/s del sistema.
- Posibilidad de ser montado sobre diferentes gestores de bases de datos.
- Bases de datos encriptadas, para evitar el acceso indeseado a los datos.
- Diferentes niveles de acceso (mediante palabra clave) configurables por usuario.
- Búsqueda de personas, para ubicar a cualquier usuario dentro del área protegida.

- Completo Gestor de Reportes, que permite ver por pantalla, imprimir o exportar a formatos estándar los datos solicitados (el mismo cuenta con diferentes criterios de filtrado para seleccionar los datos).
- Desencadenadores (triggers) y antipassback programables.
- Captura y almacenamiento de fotos digitales de usuarios.
- Monitoreo mediante fotos On-Line de accesos con cámara digital.
- Posibilidad de conexión con diferentes tipos de controladores de hardware.
- Estructura modular, que permite expandir las capacidades del sistema de acuerdo a la aplicación.
- Software, manuales y ayuda On-Line en castellano.

2.2. Estructura

En la figura 2.1 se puede ver la estructura general del NeoLock. Los componentes básicos del mismo son el servidor de comunicaciones (CommSvr) y el cliente de monitoreo, control y configuración (Control). Además, y como se verá más adelante en este manual, es posible expandir el sistema adicionando *módulos* (en la figura se pueden apreciar el Visitas.exe y el Personal.exe), los cuales también actúan como clientes del CommSvr.

La función básica del CommSvr es centralizar todas las comunicaciones con la red de paneles controladores. Realiza también ciertas operaciones, como el procesamiento del sistema de desencadenadores (triggers) y antipassback (ver [Capítulo 5: Funciones Avanzadas](#)).

El Control, en cambio, es la interfaz del usuario. El mismo permite monitorear, configurar y controlar a los paneles controladores mediante un amigable entorno gráfico. El Control es, por lo tanto, un programa “cliente” del servidor de comunicaciones.

El NeoLock se presenta básicamente en dos versiones, las cuales se describen a continuación.

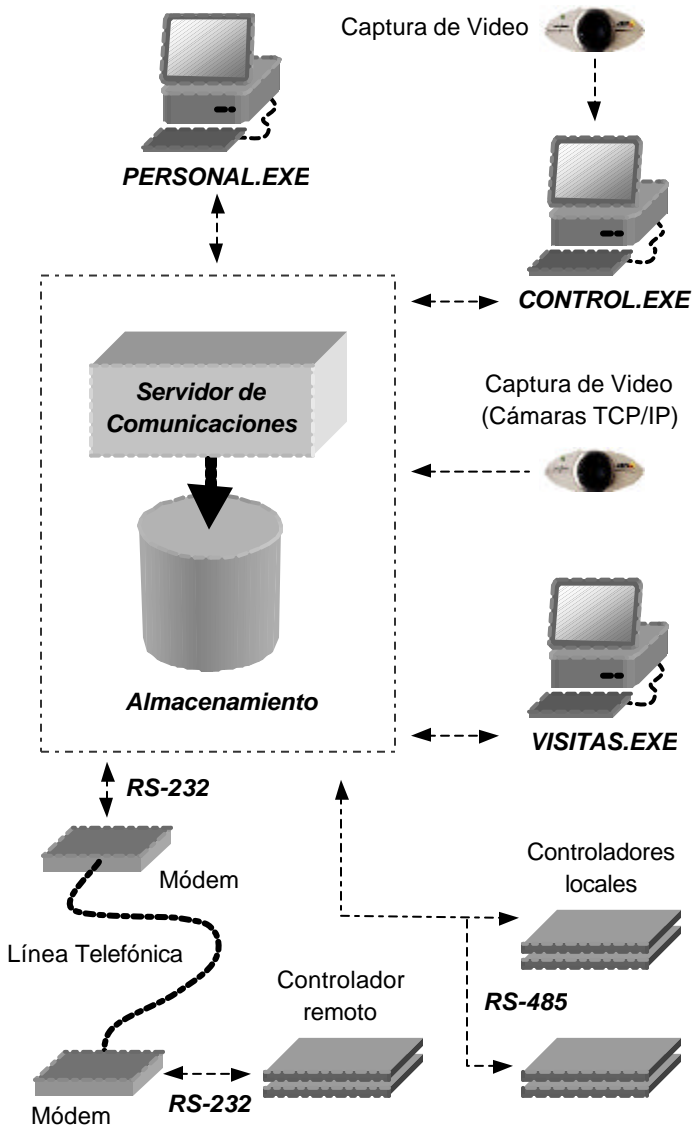


Figura 2.1. Estructura general del sistema NeoLock.

2.2.1. Versión monousuario

Para aquellos sistemas donde se centraliza todo el control y monitoreo en una sola computadora, la versión monousuario es la adecuada. Se pueden conectar todos los paneles controladores necesarios, pero sólo se accede a ellos desde una computadora. En ésta residen, por lo tanto, el servidor de comunicaciones (CommSvr) y los programas cliente (Control, Visitas, Personal, etc.). En la mayoría de las instalaciones monousuario la base de datos también se encuentra en un disco local de dicha computadora. Sin embargo, dependiendo de la estructura de la instalación, la base de datos puede residir en otra computadora conectada en red con aquella en la que se encuentra el NeoLock. La figura 2.2 muestra la estructura básica de una instalación monousuario.

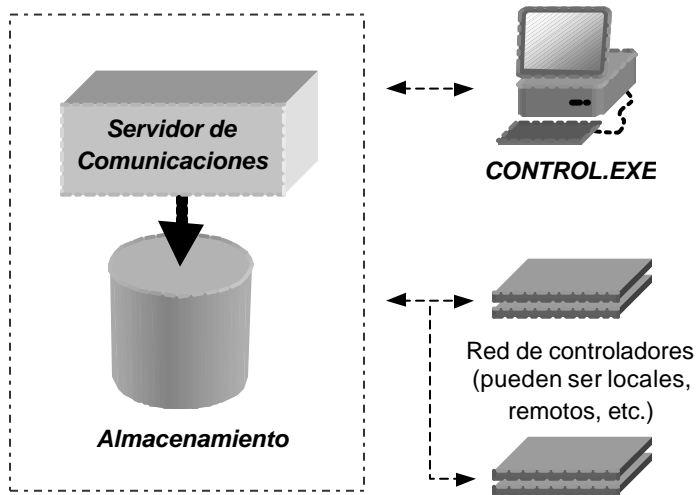


Figura 2.2. Estructura general de una instalación de NeoLock monousuario.

2.2.2. Versión multiusuario

La versión Multiusuario de NeoLock brinda la posibilidad de acceder a al sistema desde múltiples terminales. Es así como los distintos programas cliente (Control, Visitas, Personal, etc.) pueden funcionar simultáneamente en diferentes computadoras, accediendo todos al servidor de comunicaciones (CommSvr). La figura 2.3 muestra la estructura básica de una instalación multiusuario.

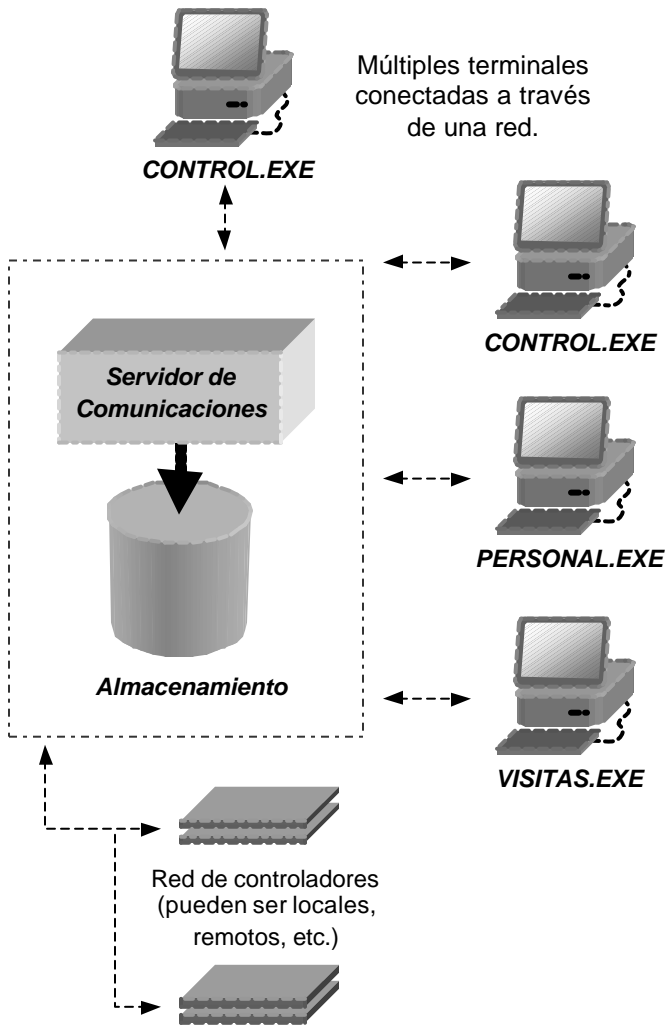


Figura 2.3. Estructura general de una instalación de NeoLock multiusuario.

2.3. Gestores de bases de datos

Independientemente de la versión de NeoLock (multi o monousuario), es necesario mantener una base de datos centralizada del sistema. En ésta se almacena, entre otros datos, la siguiente información:

- Categorías, usuarios y permisos de acceso.
- Estructura del hardware instalado (puertos, paneles, alarmas, etc.).
- Registro histórico de todos los eventos ocurridos.
- En sistemas con Módulo de Visitas, registro histórico de todos los visitantes.
- En sistemas con Módulo de Personal, registro histórico de turnos y horas trabajadas, así como horarios de trabajo, feriados, etc..

Para el almacenamiento de los datos, el NeoLock puede trabajar con diferentes gestores de base de datos estándar, como ser Paradox, SQL Server, etc. Consulte a su proveedor o directamente a ADV Technology S.R.L. por información al respecto.

2.4. Módulos adicionales y capacidad de expansión

La estructura ampliable del NeoLock permite integrar a él distintos *módulos*, según cada aplicación lo requiera. Cada uno de éstos toma la información de la base de datos del NeoLock. A continuación se da una pequeña descripción los principales módulos disponibles (cada módulo cuenta con un manual propio donde se lo describe en detalle). Es posible, por otro lado, hacer nuevos desarrollos a medida para aplicaciones específicas.

2.4.1. Módulo de Visitas

El Módulo de Visitas es un completo programa para el control de visitantes temporales. Incluye características como la captura de fotos, la categorización de visitantes, y la relación de los mismos con la persona/entidad que están visitando. También cuenta con baja automática de permisos de acceso (cuando sale el visitante), entre otras

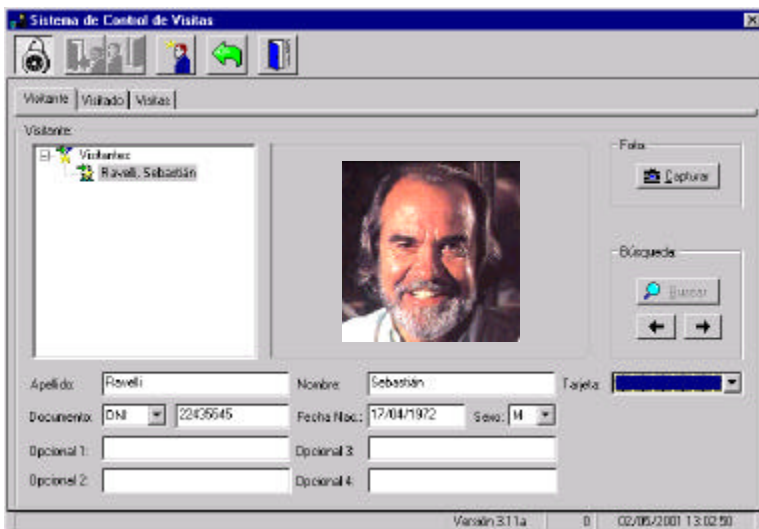


Figura 2.4. Módulo de Visitas.

facilidades. La figura 2.4 muestra una de sus pantallas. Para más información sobre este módulo, consulte el manual del Módulo de Visitas (Ref.: ADV_NK0004).

2.4.2. Módulo de Personal

Para el cómputo de horarios de trabajo, el sistema cuenta con el Módulo de Personal. El mismo soporta horarios rotativos sin límite de tiempo, procesamiento de feriados configurable, horas extras, fichadas manuales y cálculo de horas con valores porcentuales definibles. Este módulo puede ser configurado, además, para procesar sólo las fichadas que se produzcan sobre determinadas puertas del sistema de control de accesos, lo que facilita la integración sobre sistemas instalados con anterioridad a la incorporación del módulo en cuestión. Para más información sobre el mismo, consulte el manual del Módulo de Personal (Ref.: ADV_NK0005).

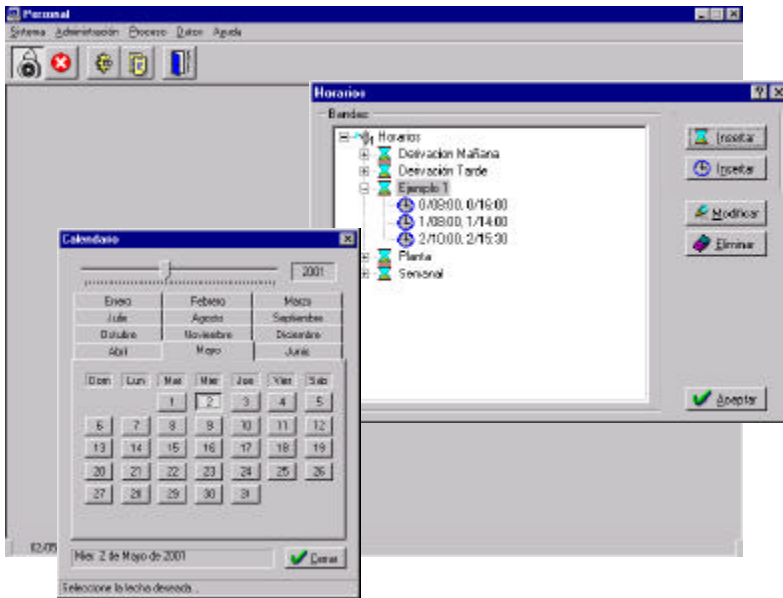


Figura 2.5. Módulo de Personal.

2.4.3. IOServer

Para el ingreso masivo de datos desde otras bases, o desde aplicaciones de planilla de cálculo, etc., existe un módulo llamado IOServer. Éste cuenta con capacidad no sólo para importar/exportar datos de la base de datos del NeoLock, sino que además puede enviar comandos (permisos, por ejemplo) a través de la red de paneles. Para más información sobre este módulo, consulte el manual del IOServer (Ref.: ADV_NK0006).

2.4.4. Desarrollos a medida

Si su aplicación requiere de características especiales que no se encuentren contempladas en el sistema o en alguno de los módulos disponibles, ADV Technology S.R.L. brinda la posibilidad de realizar desarrollos a medida. Para obtener más información acerca de esta opción, consulte a su distribuidor.

2.5. Requerimientos del sistema

Para instalar y utilizar el sistema NeoLock, necesitará:

<i>Mínimo</i>	<i>Recomendado</i>
Procesador Pentium de 100 Mhz o equivalente.	Procesador Pentium II de 333 Mhz o equivalente.
32 Mb RAM (para una configuración básica)	64 Mb RAM (128 Mb en instalaciones bajo SQL Server)
Placa de video SVGA de 1Mb	Placa de video SVGA de 4Mb
Disco rígido con 20 Mb libres. ¹	Disco rígido con 100 Mb libres. ¹
Mouse.	Mouse.
Disquetera de 3 ½".	Disquetera de 3 ½".
Un puerto serie (RS-232) libre.	Un puerto serie (RS-232) libre.
Un puerto paralelo (puede ser compartido con la impresora u otros dispositivos).	Un puerto paralelo (puede ser compartido con la impresora u otros dispositivos).
Windows 95. ²	Windows NT (WorkStation). ²

NOTAS:

1. El espacio libre de disco rígido solicitado es simplemente para la instalación inicial. Cabe destacar, que a medida que la cantidad de datos del sistema crezca (más usuarios, nuevos paneles, eventos, fotos de visitas, etc.), el espacio requerido se incrementará proporcionalmente. Además, el espacio es dependiente de la cantidad de módulos adicionales que se puedan agregar, así como del gestor de base de datos seleccionado.
2. Para los sistemas con más de 2 paneles, se recomienda una computadora dedicada al sistema NeoLock, corriendo bajo Windows NT.
3. No hay ningún inconveniente si se utilizan configuraciones superiores a la recomendada.

3. Instalación

En este capítulo se describen los pasos a seguir para la correcta instalación del sistema NeoLock. Tenga en cuenta que el orden en el que aparecen es el orden en el que deben realizarse.

3.1. El paquete NeoLock

Antes de comenzar, verifique que el paquete NeoLock incluya los siguientes elementos:

- Dos (2) discos de instalación del gestor de base de datos (Borland Database Engine, o BDE).
- Ocho (8) o más discos de instalación del software NeoLock y sus módulos (de acuerdo a la versión adquirida) o 1 CD, si se elige este medio de distribución.
- Llave de protección del software.
- Tarjeta de garantía.
- Documentación impresa (este manual y el de los módulos que corresponda, de acuerdo a la versión adquirida).

3.2. Conexión de la llave de protección

El sistema NeoLock está protegido con una llave de protección de software. Si la llave que fue provista en el paquete, no está conectada en un puerto paralelo de su PC, entonces *ningún* componente del sistema se ejecutará correctamente.

La presencia de la llave de protección es transparente para cualquier componente de hardware y/o software que posea su computadora. Para conectar la llave siga los siguientes pasos:

1. Apague la PC.

2. Si posee una impresora u otro dispositivo conectado al puerto paralelo, apáguelo y desconéctelo del puerto. Si no, saltee este paso.
3. Conecte la llave al puerto paralelo de la impresora. El extremo de la llave que se conecta con el puerto está rotulado como ^COMPUTER^.
4. Ajuste los tornillos de la llave para asegurar la misma apropiadamente al puerto.
5. Si había una impresora u otro dispositivo conectado al puerto paralelo, conecte el cable del mismo al conector externo de la llave de protección. Si no, saltee este paso.

3.3. Programas instaladores

Dependiendo del sistema que haya adquirido, es posible que durante su instalación, deba correr más de un programa instalador. En esta sección se explica de una manera gráfica, el procedimiento general para ejecutar un instalador bajo Windows. En las siguientes secciones, por lo tanto, sólo se hará mención de qué programa instalador debe ejecutarse, sin volver a enumerarse todos los detalles aquí expuestos. Para correr un programa instalador en Windows existen varias posibilidades. A continuación describiremos dos formas de hacerlo.

NOTAS:

1. A lo largo de todos los ejemplos de instalación, se asume que se trabaja con una distribución de NeoLock en discos de 3 ½" pulgadas. Es posible que su distribución sea en CD, en cuyo caso deberá consultar las instrucciones distribuidas con el paquete adquirido. En caso de tratarse, por otro lado, de una distribución vía Internet, la misma contendrá instrucciones de instalación en formato electrónico.
2. Para los ejemplos se asume que la disquetera utilizada tiene la letra de unidad **A:**.
3. Si está trabajando sobre Windows NT, antes de correr cualquier programa de instalación relacionado con el

sistema NeoLock, debe iniciar la sesión como **Administrador (Administrator)**, en las versiones en inglés). Si no puede hacerlo por los permisos de que dispone, consulte al administrador de su red o sistema, para efectuar esta operación. No se asegura el funcionamiento correcto de ninguno de los componentes si no son instalados por el usuario Administrador.

3.3.1. Utilizando el explorador de Windows.

Supongamos que queremos ejecutar un programa llamado **INSTALAR.EXE**, el cual, como ocurrirá en todos nuestros ejemplos, se encuentra en la disquetera denominada **A:**.

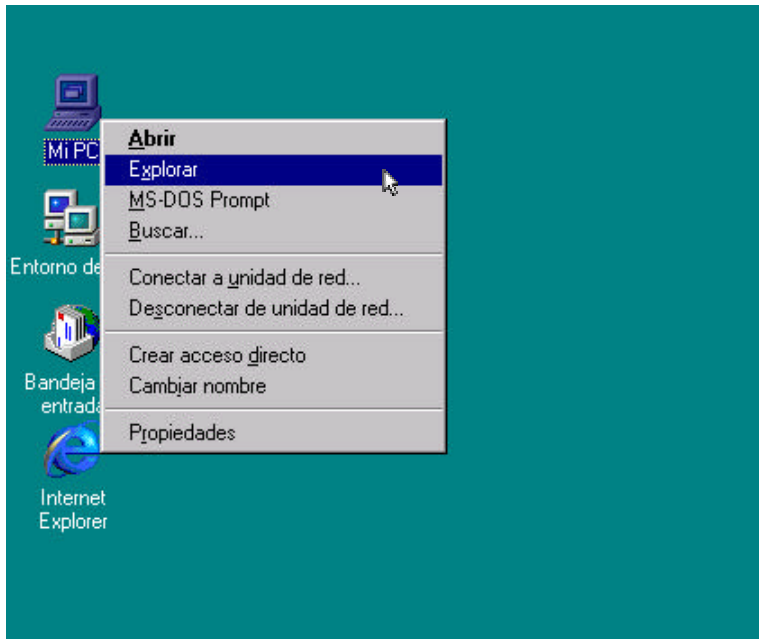


Figura 3.1. Abriendo el explorador de Windows.

Los siguientes pasos muestran cómo correrlo utilizando el explorador de Windows.

1. Abra el explorador. Una forma de hacer esto es posicionarse con el mouse sobre el ícono **Mi PC** (el cual se encuentra en el escritorio de Windows), presionar el botón derecho y seleccionar la opción **Explorar** del menú desplegable (figura 3.1). En las versiones de Windows en inglés, el ícono se llamará **My Computer**, y la opción del menú será **Explore**.
2. Una vez abierto el explorador, haga un click sobre la disquetera 3 ½ de la parte izquierda de la ventana (figura 3.2). Deberá aparecer, en la parte derecha, el contenido del disco de instalación (siempre y cuando éste haya sido colocado correctamente en dicha disquetera).

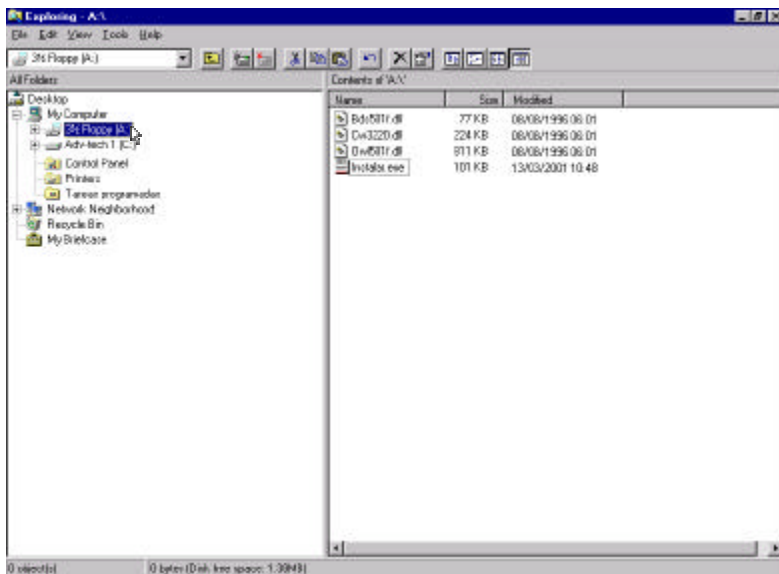


Figura 3.2. Explorador de Windows.

3. Ahora sólo resta dar doble click sobre el ícono o el nombre del programa (en nuestro ejemplo **INSTALAR.EXE**) para que éste se ejecute.

3.3.2. Desde el menú Inicio de Windows.

Otra forma de correr programas bajo Windows es mediante el menú del botón **Inicio (Start)**, si su sistema operativo está en inglés). Para el ejemplo anterior, los pasos serían los siguientes:

1. Haga click con el mouse sobre el botón **Inicio (o Start)** en inglés).
2. Del menú desplegable, seleccione **Ejecutar (Run)**, como se ve en la figura 3.3.

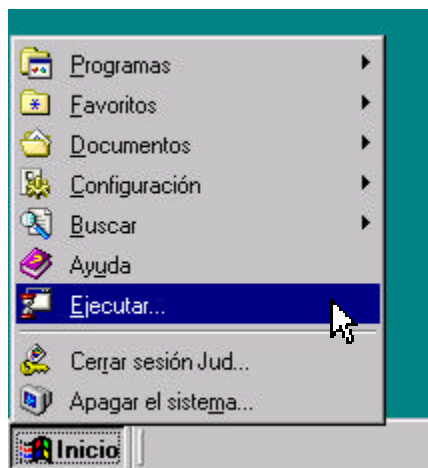


Figura 3.3. Menú Inicio.

3. Se desplegará la ventana de la figura 3.4, en la cual puede ingresar directamente la ruta de acceso al programa que queremos ejecutar (en el ejemplo es **A:\INSTALAR.EXE**). También puede presionar el botón **Examinar (Browse)**, en inglés) para buscar dicho archivo.
4. Haga click sobre el botón **Ok** de la ventana antedicha, y el programa comenzará a ejecutarse.

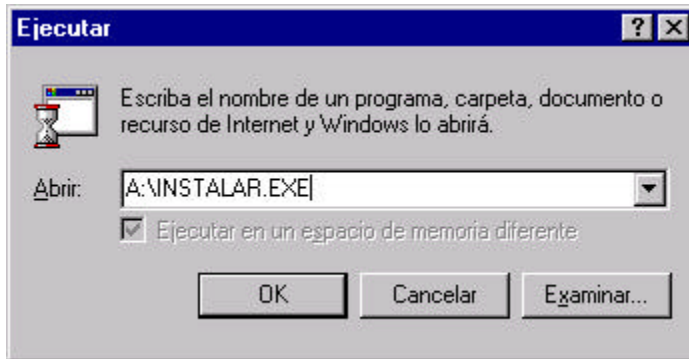


Figura 3.4. Ventana para ejecutar programas bajo Windows.

Cualquiera de estas dos sencillas formas puede ser utilizada para correr los programas instaladores que se utilizarán durante la instalación.

3.4. Instalación del gestor de base de datos BDE

Éste es el primer paso en la instalación del software. Independientemente del gestor de base de datos seleccionado, el BDE debe ser instalado, pues es una parte constituyente del sistema. Dos de los discos de instalación provistos con el paquete están rotulados como **Gestor de Base de Datos**. En el primero de ellos se puede encontrar el programa instalador llamado **SETUP.EXE** (para correrlo, consulte la [sección 3.3 Programas Instaladores](#)). Al ejecutarlo, aparecerá por unos segundos la pequeña ventana de la figura 3.5, la cual le informa que el programa se está preparando para la instalación.

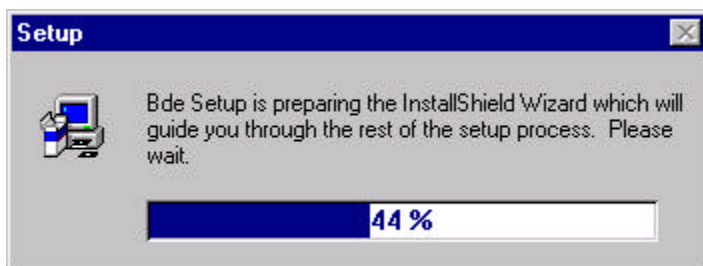


Figura 3.5. Ventana temporal del instalador del BDE.

La figura 3.6 muestra la primer pantalla que se desplegará luego. Haga click con el mouse sobre el botón **Next >**, para pasar a la ventana de la figura 3.7. Si en algún momento desea cancelar la instalación, haga click sobre el botón **Cancel** (aparecerá entonces una pequeña ventana, en la que deberá dar click sobre el botón **Exit Setup**).

En la ventana de la figura 3.7, ingrese el nombre del usuario

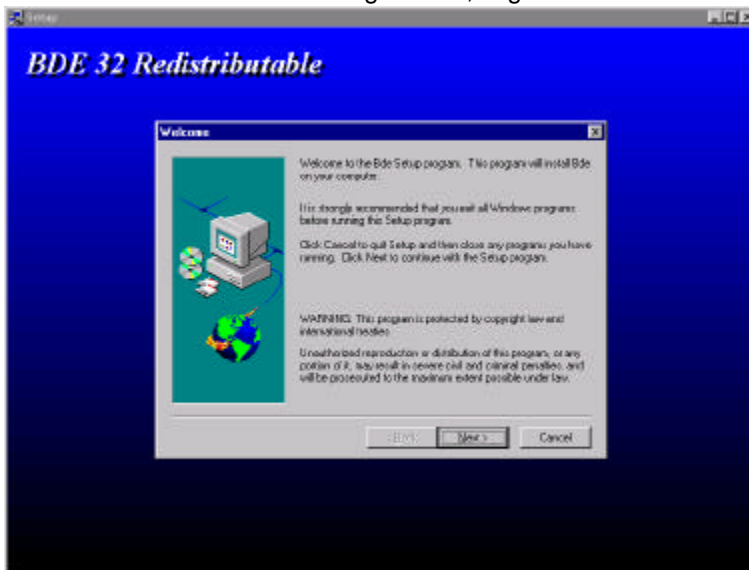


Figura 3.6. Programa instalador del BDE.

(**Name**) y de la empresa (**Company**) que corresponda y presiones **Next >**.

La siguiente ventana será la de la figura 3.8 En ella puede ingresar la ruta de destino donde desea que el BDE se instale.

NOTA:

No es recomendable que cambie la ruta de destino presentada por defecto por el instalador.

En las ventanas que aparecerán de aquí en más, lo recomendado es que presione **Next >** hasta que el instalador comience a copiar los archivos.

En algún momento durante la copia de archivos, el programa le solicitará que inserte en la disquetera el disco de instalación 2. El mensaje que usted verá en ese momento será: **"Setup needs the next disk"**. Simplemente reemplace el disco y presione el botón **Aceptar**.

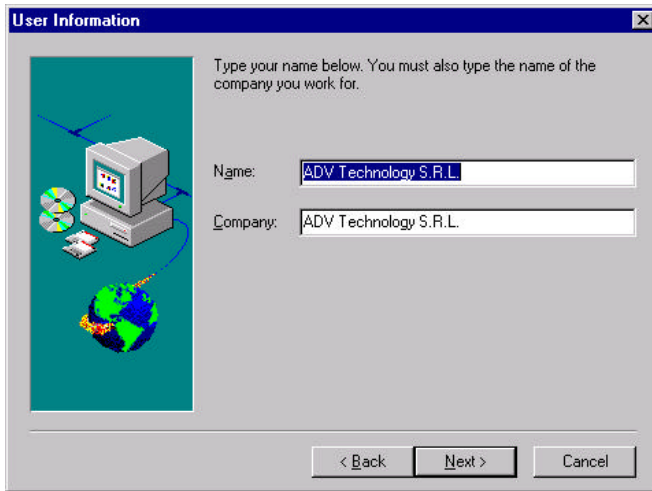


Figura 3.7. Datos del usuario y la empresa.

En la última ventana aparecerá el botón **Finish**. Al darle click a este botón habrá terminado la instalación del BDE.

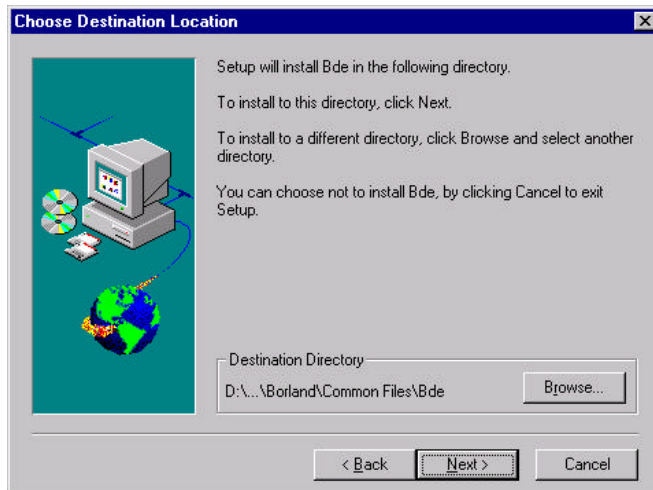


Figura 3.8. Ruta de destino para la instalación del BDE.

3.5. Instalación del sistema NeoLock

3.5.1. Instalación básica

En el primer disco de instalación del NeoLock se puede encontrar el programa instalador llamado **NEOINST.EXE** (para correrlo, consulte la [sección 3.3 Programas Instaladores](#)). Al ejecutarlo, aparecerá la ventana de la figura 3.9.

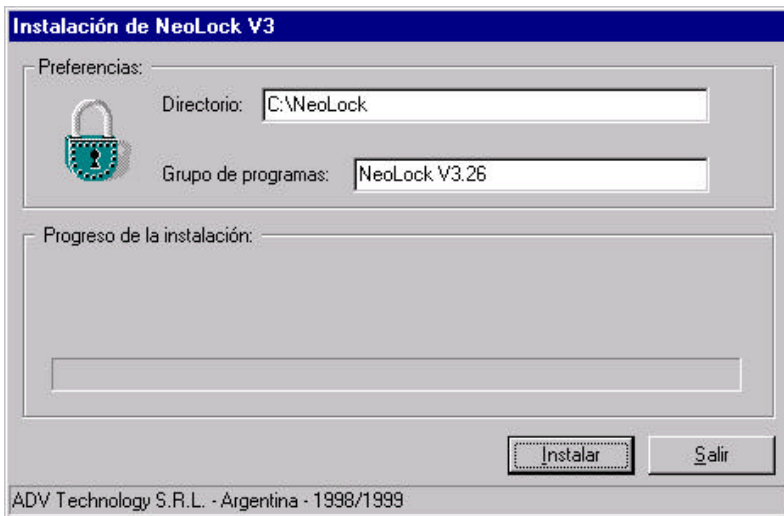


Figura 3.9. Ventana del programa instalador de NeoLock (NEOINST.EXE).

En la entrada de texto denominada como **Directorio**, debe especificar la ruta completa de acceso al directorio de destino donde desea instalar el sistema. Si el directorio ingresado no existe, el programa de instalación lo creará. En cambio, si ya existe, el instalador sobrescribirá su contenido, por lo que se perderán los datos. Si desea instalar, por lo tanto, en un directorio existente, asegúrese de hacer una copia de todos los datos.

En la otra entrada de texto (**Grupo de programas**), puede ingresar el grupo que será creado en el menú **Programas** del botón **Inicio** de Windows para acceder al soft.

Una vez ingresados estos datos, presiones el botón **Instalar**. Esto dará comienzo a la copia de archivos y a la instalación de todos los

componentes del sistema (previamente se desplegará una pequeña ventana de confirmación, en la que deberá presionar el botón **Si** para proseguir con la instalación). Si en algún momento desea abandonar la instalación, presione el botón **Salir**.

Cuando el instalador concluya, aparecerá en pantalla la ventana de la figura 3.10.

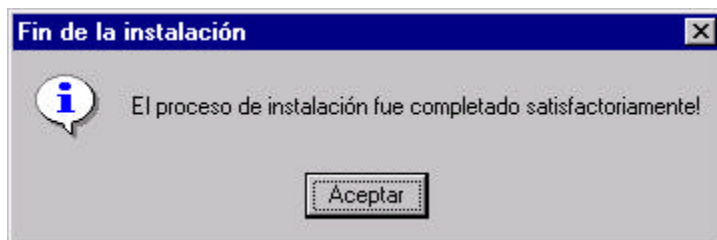


Figura 3.10. Ventana de finalización del programa instalador de NeoLock.

Presione el botón Aceptar y luego el botón Salir. Ahora los componentes del sistema han sido instalados.

Antes de comenzar a utilizar el NeoLock, **deberá reiniciar la PC**. Esto concluye el proceso de instalación.

NOTAS:

1. Usted sólo necesita correr el instalador **una** vez. Si éste es ejecutado más de una vez, entonces usted tendrá íconos duplicados en el grupo NeoLock.
2. Si durante la instalación se produce algún error, la aplicación desplegará un mensaje informándole lo ocurrido.

3.5.2. Sistemas monousuario

En un sistema monousuario, el paso descrito en la sección anterior ([Instalación básica](#)), finaliza la instalación.

Si se completó dicha etapa con éxito, una vez reiniciada la PC, ya puede comenzar a hacer uso de su sistema NeoLock.

3.5.3. Sistemas multiusuario

En un sistema multiusuario típico, una computadora (a la que llamaremos **servidor** a lo largo de este documento) centralizará las comunicaciones con los paneles controladores y el almacenamiento de los datos en la base. Es en esta computadora, donde debe instalarse el programa llamado servidor de comunicaciones (COMMSVR.EXE). Los programas de configuración y monitoreo (como el CONTROL.EXE) y los otros módulos (como el Módulo de Visitas, o el de Personal) pueden ser instalados tanto en el servidor como en distintas **terminales** conectadas al mismo a través de una red. A continuación se enumeran los pasos a seguir para instalar el servidor:

1. Cree manualmente el directorio de instalación del NeoLock en la computadora que funcionará como servidor.
2. Comparta el directorio de instalación, de modo que las terminales puedan acceder al mismo a través de la red.
3. Mapee una unidad de red sobre el directorio de instalación. Marque la casilla “Volver a conectar al inicio de sesión” (o “Reconnect at logon” en la versión en inglés). La letra con la que designe a la unidad no deberá estar en uso en la red (ni en el servidor ni en las terminales).
4. Instale el NeoLock sobre la unidad de red mapeada en el paso 3. Para esto, debe realizar las operaciones descritas en la [sección 3.5.1: Instalación Básica](#), colocando como directorio de instalación directamente al directorio raíz de la unidad de red.

La instalación en las terminales depende de las características del sistema particular, por lo que se recomienda consultar a su proveedor o directamente a [ADV Technology S.R.L.](#) (vea también la sección [Soporte técnico](#)). Básicamente, cada terminal debe tener instalados el [Gestor de base de datos BDE](#) y el driver de la llave de hardware, y creados accesos directos a los ejecutables que residen en el servidor.

3.6. Instalación de módulos adicionales

Durante la [instalación básica](#), el programa instalador copia los archivos correspondientes a los siguientes módulos adicionales (como

cada módulo cuenta con su propia documentación, la tabla indica la referencia del manual de cada módulo):

<i>Módulo</i>	<i>Documentación</i>
Módulo de Visitas	Ref.: ADV_NK0004
Módulo de Personal	Ref.: ADV_NK0005
IOServer	Ref.: ADV_NK0006

Para utilizar cada uno de éstos módulos, deberá adquirir la licencia correspondiente, con la cual será habilitada su llave de protección para poder hacer uso de dicho módulo.

NOTA:

En el subdirectorio **Docs** del directorio donde fue instalado el sistema NeoLock, encontrará documentación en formato electrónico (archivos PDF).

3.7. Sistemas con otros gestores de base de datos

El gestor de base de datos utilizado por defecto por el NeoLock es el BDE. Si ha elegido otro gestor para administrar su base de datos de NeoLock, debe instalarlo correctamente antes de poder utilizar el sistema. Como se mencionó antes, aunque se trabaje con otro sistema de base de datos, el BDE debe ser instalado de todas maneras, ya que es parte constituyente del NeoLock. Para obtener detalles acerca de la instalación de otros gestores de base de datos, y de versiones de NeoLock para trabajar con los mismos, consulte a su distribuidor o directamente ADV Technology S.R.L..

El manual Ref.: ADV_NK0010, titulado “Instalación de Terminal NeoLock bajo SQL Server” brinda información útil a este respecto, para sistemas corriendo sobre MS SQL Server.

4. Funcionamiento y estructura básicos

4.1. Inicio de la aplicación

Al instalar el software, será creado un grupo llamado NeoLock dentro del menú Programas (Programs, en las versiones de Windows en inglés) del botón Inicio (Start). En éste se podrán encontrar los accesos directos para el NeoLock (CONTROL.EXE), el Servidor de Comunicaciones (COMMSVR.EXE) y los módulos de Visitas, Personal e IOserver (VISITAS.EXE, PERSONAL.EXE e IOSERVER.EXE, respectivamente). Hay además un acceso directo al subdirectorío DOCS, que contiene documentación del sistema en formato electrónico (archivos para Acrobat Reader, con extensión PDF) y un acceso a la Ayuda en Línea del NeoLock.

4.1.1. Cómo ingresar al sistema por primera vez

Al ejecutar el acceso directo llamado NeoLock, se iniciarán automáticamente el Servidor de Comunicaciones y el programa de monitoreo y configuración (CONTROL.EXE). Una vez que éste último se ejecutó, vaya al menú **Seguridad** y haga click en la entrada de menú **Iniciar Sesión** (figura 4.1).

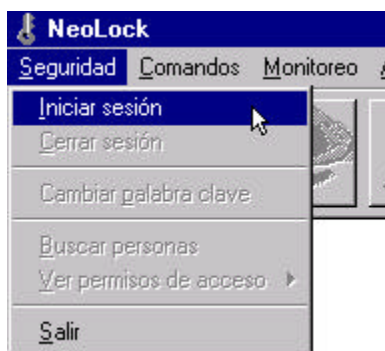


Figura 4.1. Menú Seguridad del NeoLock.

Aparecerá la ventana de la figura 4.2. En ella se solicita al usuario que ingrese su identificación y su palabra clave. El único

usuario existente luego de la instalación, es el **Administrador del Sistema**. Su identificación es la letra **a**, al igual que su palabra clave. Tenga en cuenta que la palabra clave es la letra **a** minúscula, por lo

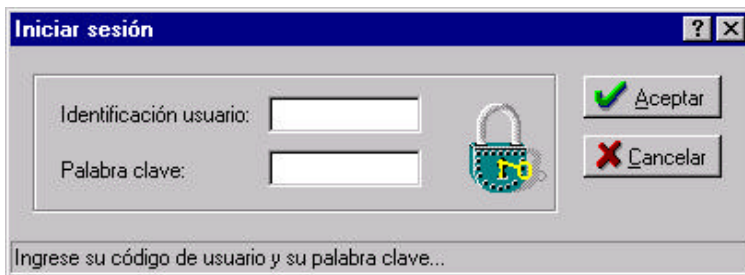


Figura 4.2. Ventana de Inicio de Sesión del NeoLock.

que, en caso de que el sistema no le permita iniciar la sesión, verifique que su teclado no tenga encendido el indicador de Mayúsculas (Caps Lock, en teclados en inglés).

NOTA:

Es altamente recomendable cambiar la palabra clave del Administrador de Sistema la primera vez que se ingresa al NeoLock, para evitar accesos futuros indeseados.

4.2. Configuración del sistema

Una vez que ha instalado el NeoLock e ingresado al mismo ([sección 4.1.1](#)), puede darse comienzo a su configuración.

Configurar el sistema consiste en ingresar la información necesaria para que el mismo funcione correctamente. Esta información incluye, básicamente, la estructura de la red física de paneles controladores, los datos de los usuarios y los permisos de accesos por usuario, con sus respectivos horarios de habilitación. Existen otros tópicos más avanzados relativos a la configuración, los cuales se tratan a partir del [capítulo 5 \(Funciones Avanzadas\)](#). En las secciones subsiguientes se describirá la configuración básica.

4.3. Estructura y configuración del hardware

El primer paso en la configuración del sistema es ingresar los datos de la estructura de hardware (red de paneles controladores) que deberá controlar.

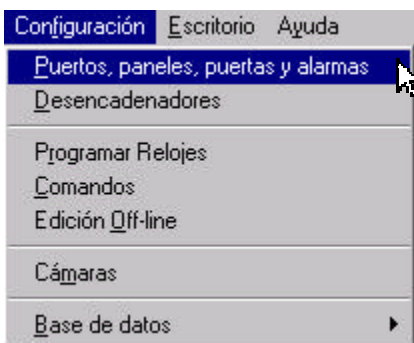


Figura 4.3. Menú Configuración.

Para dar comienzo a esta operación, vaya al menú **Configuración** y haga click en la entrada de menú **Puestos, paneles, puertas y alarmas** (figura 4.3). Se desplegará la ventana de la figura 4.4.

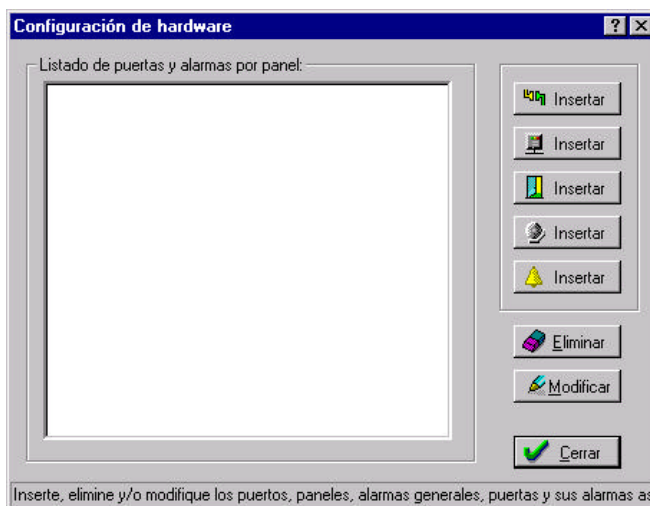


Figura 4.4. Ventana de configuración del hardware.

4.3.1. Puertos de comunicaciones

El primer paso al generar la estructura de hardware del sistema es crear él o los puertos de comunicaciones. Todo panel controlador debe estar conectado a un puerto para poder comunicarse con la PC. Existen diferentes formas de conectar los paneles, que serán descritas en esta sección. Para crear un puerto haga click en el primer botón titulado **Insertar** de la ventana de configuración de hardware (figura 4.4). Aparecerá la ventana de la figura 4.5.

El primer campo de la ventana es el **Nombre** que se le dará al

The image shows a Windows-style dialog box titled "Configuración del Puerto". It is divided into three main sections: "Propiedades", "Servidor Principal", and "Servidor Secundario".
- In the "Propiedades" section, there is a text field for "Nombre" containing "Nuevo Puerto" and a dropdown menu for "Tipo de Conexión" set to "RS-232/RS-485".
- In the "Servidor Principal" section, there is a dropdown for "Computadora" set to "NEOSERVER", and four text input fields for "Puerto 1" (containing "1"), "Puerto 2", "Puerto 3", and "Puerto 4".
- In the "Servidor Secundario" section, there is a dropdown for "Computadora" set to "No usado", and four empty text input fields for "Puerto 1", "Puerto 2", "Puerto 3", and "Puerto 4".
At the bottom of the dialog are three buttons: "Buscar" (with a magnifying glass icon), "Aceptar" (with a green checkmark icon), and "Cancelar" (with a red X icon).

Figura 4.5. Ventana de configuración de puerto.

puerto. El mismo no puede tener más de 30 caracteres.

El segundo campo es el **Tipo de Conexión**. Allí se le presentarán 4 opciones, dependiendo del tipo de comunicaciones que utilice para conectar los paneles. Más adelante se describen todas ellas.

El campo titulado **Computadora**, es donde se especifica el nombre de red del equipo que corra al Servidor de Comunicaciones (COMMSVR.EXE). El sistema NeoLock listará automáticamente todos los equipos que encuentre en su dominio. Si quiere hacer una búsqueda más allá del dominio de equipos, utilice el botón **Buscar** de la

parte inferior de la ventana. Tenga en cuenta que esta operación de búsqueda puede tardar desde algunos segundos hasta varios minutos, dependiendo de la estructura de la red.

4.3.1.1. RS-232/RS-485

Si se tiene una instalación con un solo panel, conectada vía puerto serie (RS-232) con una PC, como muestra la figura 4.6, debe seleccionar esta opción. Para concluir la configuración de un puerto de este tipo, sólo falta que seleccione el nombre de la computadora que tiene el puerto RS-232 (campo **Computadora** de la ventana de la figura 4.5) y el número de puerto a utilizar. Dicho número se ingresa en el

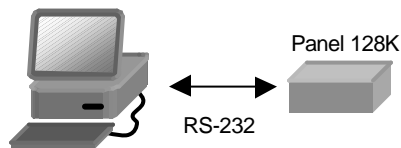


Figura 4.6. Conexión vía RS-232 de un panel controlador con la PC.

campo titulado **Puerto 1** de la misma ventana (un 1 corresponderá al COM1, un 2 al COM2, y así sucesivamente).

En el caso de disponga de una red de paneles controladores conectados a la PC mediante un bus RS-485 y un conversor RS-232/RS-485 (figura 4.7), la configuración del puerto es exactamente

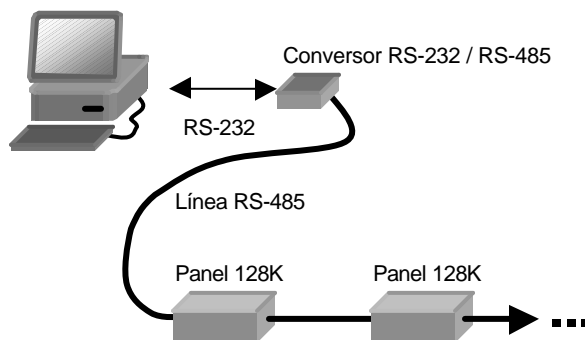


Figura 4.7. Conexión de una red de panel controladores y una PC mediante un bus RS-485.

igual: simplemente seleccione la PC y el puerto serie utilizados.

4.3.1.2. Módem

En instalaciones con paneles remotos, controlados vía línea telefónica (figura 4.8), debe seleccionar la opción **Módem** para el **Tipo de Conexión**.

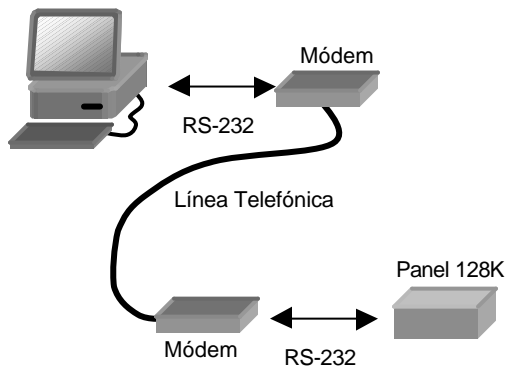


Figura 4.8. Conexión de paneles remotos mediante línea telefónica y módems.

Una característica de las conexiones telefónicas es que el servidor (la PC) llamará periódicamente a él o los paneles, por lo que la conexión no es permanente. Por otro lado, los paneles controladores pueden también discar e intentar conectarse con el servidor en determinadas circunstancias (por ejemplo frente al disparo de una alarma). Si por alguna razón la conexión telefónica no se pudiera establecer, es posible configurar un **Servidor Secundario**, con el que los paneles intentarán conectarse ante eventuales problemas con el **Servidor Principal**.

Es por esto que al seleccionar este tipo de conexión de la lista de opciones de la ventana, se habilitará automáticamente el campo **Nombre** del **Servidor Secundario**. El mismo puede no existir (aparecerá el texto "No usado" en dicho campo).

También es posible conectar más de un módem al mismo servidor (esto permite utilizar distintas líneas telefónicas con la misma PC). Simplemente ingrese el número de puerto serie (COM) al que ha

conectado él o los módems. Como verá en la ventana, puede disponer de hasta 4 módems por servidor.

4.3.1.3. MDLC Gateway

La estructura de este tipo de conexiones se muestra en la figura 4.9. Permite conectar paneles controladores mediante RF. La conexión entre la PC y el Gateway RF es TCP-IP. La dirección IP se especifica en el archivo COMMSVR.INI (consulte a su distribuidor

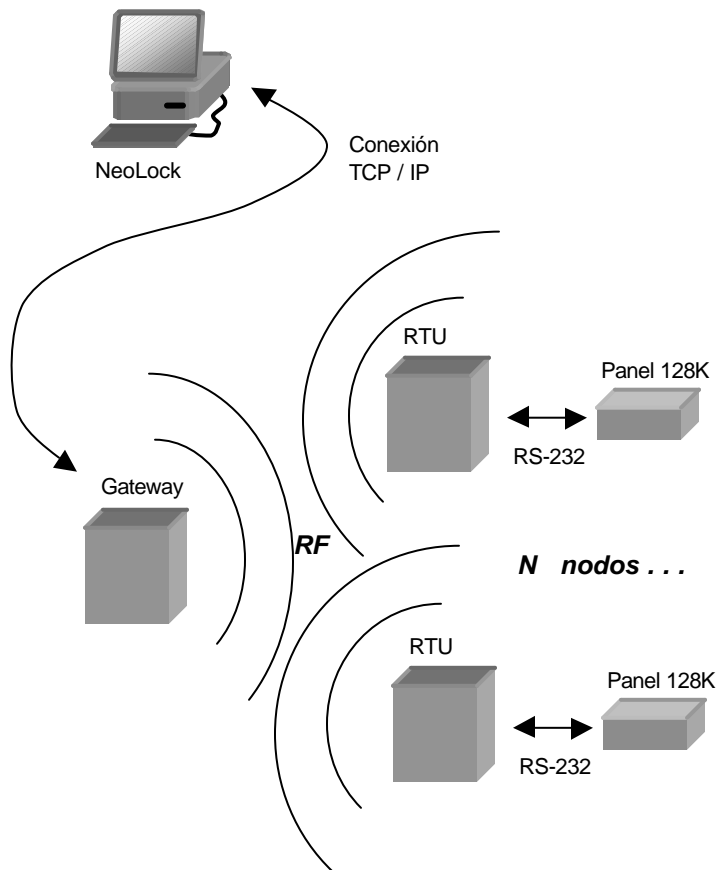


Figura 4.9. Conexión de los paneles controladores mediante Gateways RF.

autorizado a directamente a [ADV Technology S.R.L.](#) para configurar éste y otros parámetros). En el campo correspondiente al **Puerto 1** de la ventana de configuración de puertos, se ingresa el número de identificación del RTU. Éstos números son configurados en cada RTU por el instalador de los mismos.

4.3.1.4. TCP-IP

La figura 4.10 muestra cómo es posible conectar paneles controladores a PCs distribuidas a lo largo de una Intranet/Extranet, y centralizar todo el control en un servidor NeoLock.

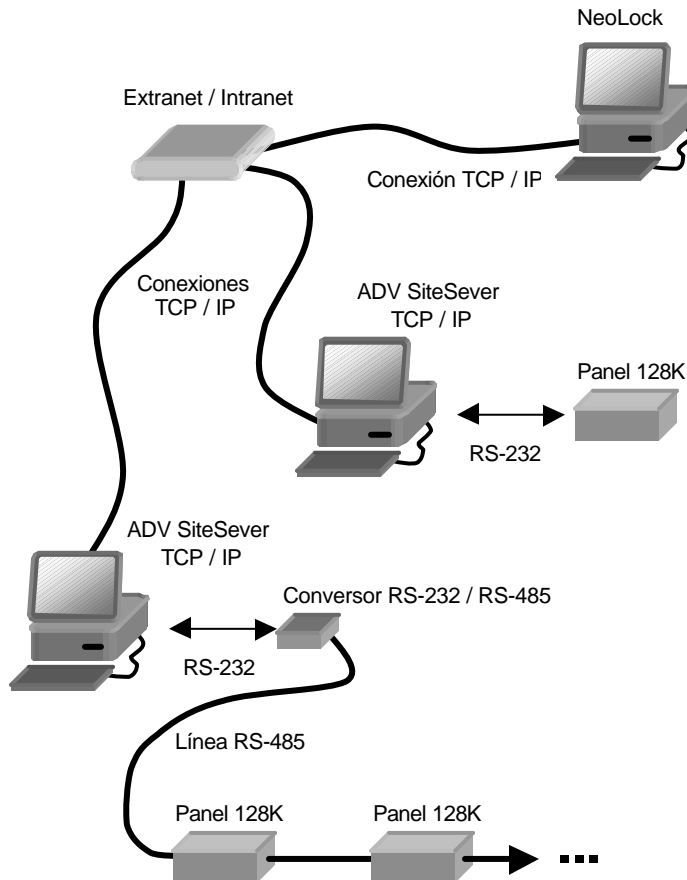


Figura 4.10. Conexión TCP-IP (vía Intranet/Extranet).

Cada PC “cliente” deberá correr un programa llamado ADV-SiteServer, el cual permite que el NeoLock envíe comandos o reciba eventos a través de la red TCP-IP a los paneles conectados a cada computadora local. La conexión entre los paneles y las PCs locales puede ser tanto RS-232 como RS-485. En el campo correspondiente al **Puerto 1**, debe ingresarse la dirección IP de la PC corriendo el SiteServer (por lo tanto, deberá crear un puerto por cada PC cliente).

4.3.2. Paneles controladores

Una vez creados él o los puertos de comunicaciones, deben ser insertados los paneles controladores conectados a éstos. Para insertar un nuevo panel, simplemente seleccione el puerto al que estará conectado, y presione el segundo botón **Insertar** de la ventana de configuración de hardware, como se muestra en la figura 4.11.

Deberá aparecer la ventana de la figura 4.12.a. A continuación

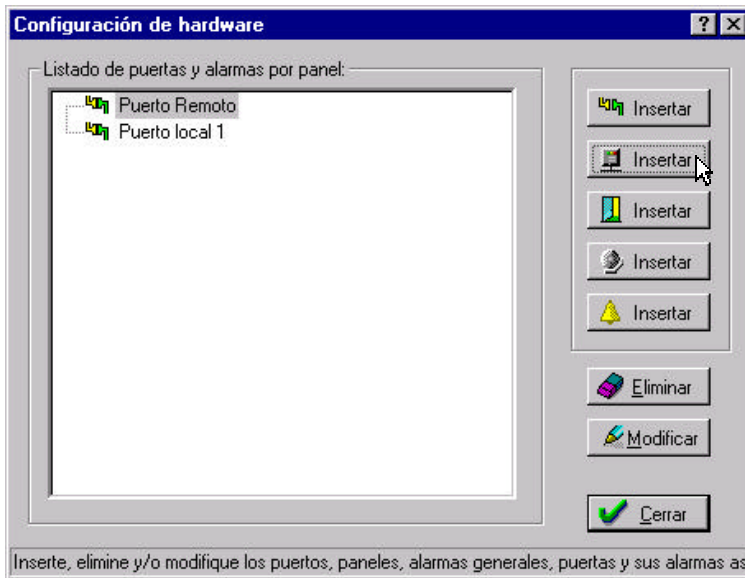


Figura 4.11. Inserción de paneles controladores.

se listan los campos de esta ventana y sus significados.

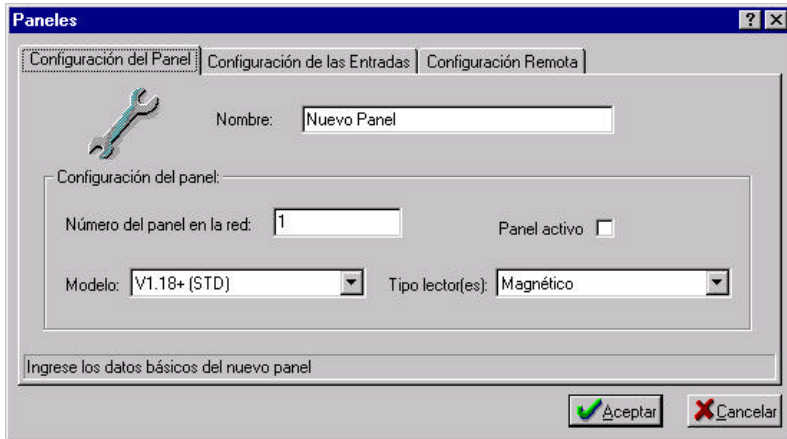


Figura 4.12.a. Ventana de edición de panel controlador (solapa “Configuración del Panel”).

- **Nombre:** Nombre que identificará al panel en el sistema. Puede contener hasta 30 caracteres.
- **Número de panel en la red:** En paneles RS-485, donde puede haber hasta 31 paneles, este número debe coincidir con el configurado en los switches del panel (consulte el Manual de Instalación del Hardware, Ref.: ADV_NK0003, para obtener más información sobre los números de panel). En paneles RS-232, aunque puede haber sólo un panel por conexión, el número debe configurarse exactamente igual a los paneles RS-485. En paneles remotos, el número no está limitado a 31, ya que puede haber tantos paneles como conexiones telefónicas.
- **Modelo:** El sistema NeoLock soporta distintos modelos de panel (no estando restringida la gama a los fabricados por ADV Technology S.R.L.). Consulte con su proveedor para ver qué modelo es el utilizado en su instalación.
- **Panel Activo:** Muchas veces es deseable hacer una serie de cambios en la configuración de un panel, o en los permisos de acceso, para luego enviarlos todos juntos al mismo. Esto agiliza la operatoria del sistema. Esta casilla

de selección permite desconectar por software al panel en cuestión, de modo que el sistema no intentará enviar los cambios inmediatamente. Note que si un panel no está On-Line tampoco se reciben sus eventos, por lo que es imprescindible seleccionar esta opción cuando se desea tener comunicación con el mismo.

- **Tipo lector(es):** Los paneles controladores de ADV Technology S.R.L. soportan tanto lectores de proximidad con norma Wiegand como ABA Track-2. La única restricción es que, si se conectan 2 lectores al panel, ambos deben ser del mismo tipo. En este campo se especifica el tipo de lector/es conectado/s al panel.

La figura 4.12.b muestra la segunda solapa de la ventana de configuración de paneles (“Configuración de las Entradas”).



Figura 4.12.b. Ventana de edición de panel controlador (solapa “Configuración de las Entradas”).

Esta ventana permite definir cuáles de las 8 entradas del panel controlador están habilitadas y cómo serán interpretados los estados de las mismas (permite seleccionar entre entradas Normal Cerradas –NC- o Normal Abiertas –NA-).

Por último, en la figura 4.12.c, se presenta la última solapa de la ventana de configuración (“Configuración Remota”). Tenga en cuenta que sólo podrá ingresar datos en sus campos si el panel en cuestión

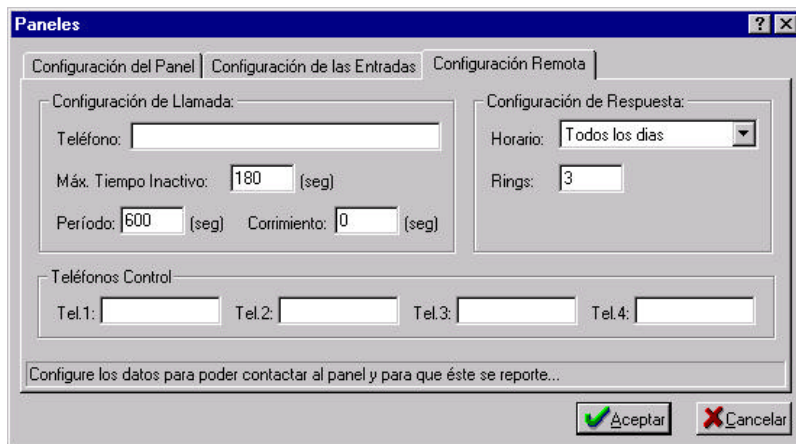


Figura 4.12.c. Ventana de edición de panel controlador (solapa “Configuración Remota”).

está conectado a un puerto remoto (módem). A continuación se describen sus campos:

- **Teléfono:** Número telefónico completo al que la PC con el Servidor de Comunicaciones llamará para comunicarse con el panel. Cada número telefónico debe estar precedido por una P o una T, mayúsculas, que indicarán si el discado será por pulsos (P) o por tonos (T). Además de éstos, se pueden especificar otros caracteres especiales (como la coma, etc.), de acuerdo a lo soportado por el módem que esté utilizando para discar (comando ATD). Consulte la documentación de su módem para mayores detalles.
- **Máx. Tiempo Inactivo:** Tiempo máximo (expresado en segundos) que el panel puede permanecer sin recibir/enviar datos por la línea telefónica antes de cortar.
- **Período:** Tiempo especificado en segundos, entre llamadas del servidor hacia el panel. Por ejemplo, un período de 600 segundos hará que la computadora (servidor) llame al panel cada 10 minutos. La hora base para el conteo del período

es 00:00 hs., aunque se puede especificar un corrimiento (vea la descripción del siguiente campo),

- **Corrimiento:** Normalmente, cada llamada del servidor hacia el panel ocurre cada vez que transcurre un tiempo igual al especificado en el campo período. Mediante el corrimiento, es posible hacer que dicho tiempo no se cuente desde las 00:00 hs., sino desde un tiempo igual a las 00:00 hs. + Corrimiento.
- **Tel. 1 – Tel. 4:** Cuando en el panel se producen ciertos eventos (como el disparo alarmas, etc.), éste puede discar y comunicarse al servidor para informarlo. Es posible configurar hasta 4 números telefónicos, de modo que si no logra establecer comunicación con el primero, intentará con el segundo y así hasta el cuarto. El formato de los números telefónicos es el mismo que en el campo teléfono.
- **Horario:** El panel controlador sólo atenderá dentro del horario especificado en este campo. El horario es un horario de NeoLock (ver [sección 4.6.1: Bandas y horarios](#)).
- **Rings:** Cantidad de rings que el panel dejará sonar antes de atender la llamada (note que sólo atenderá si está dentro del horario especificado).

NOTA:

Dependiendo del modelo de panel controlador seleccionado, puede haber variaciones en las opciones de las distintas solapas de la ventana de configuración.

4.3.3. Puertas

Es posible conectar hasta dos lectores de tarjetas de proximidad (u otro tipo de lectores o dispositivos de identificación compatibles con el sistema) a cada panel. Esto permite controlar una puerta con un lector de entrada y uno de salida, o dos puertas con un lector y un pulsador de salida (REX, -Request to EXit-) cada una.

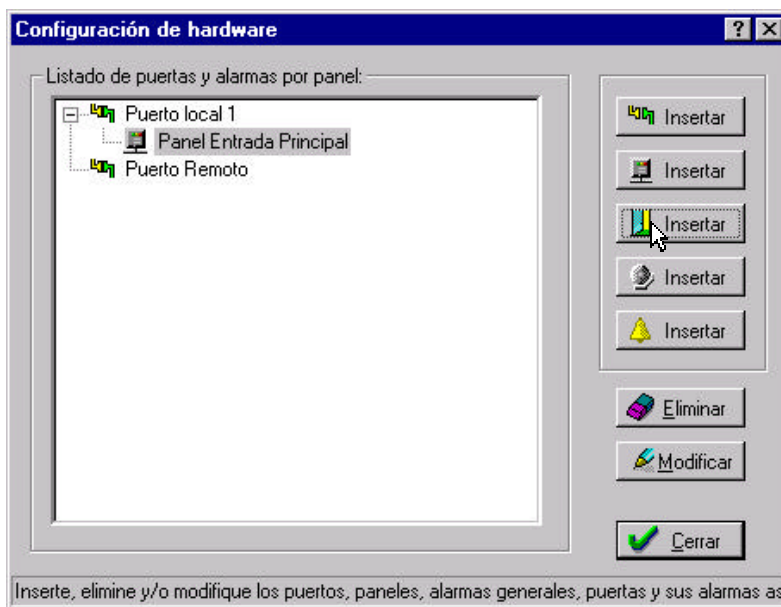


Figura 4.13. Inserción de una puerta.

En el NeoLock, esto se representa mediante la inserción de puertas en el panel controlador.

Para insertar una nueva puerta, seleccione el panel que la controlará y presione el tercer botón **Insertar** (figura 4.13).

Se desplegará la ventana de la figura 4.14.a. La primer solapa de esta ventana, llamada **Identificación**, contiene los siguientes campos:

- **Nombre:** Nombre que identificará a la puerta en el sistema. Puede contener hasta 30 caracteres.
- **Tipo:** Indica si se tratará de una puerta (incluye puertas convencionales de una hoja, puertas de 2 hojas, corredizas, etc.) o de una barrera (típicamente barreras de control vehicular). El sistema las distingue por las diferencias en la forma en que se controlan.



Figura 4.14.a. Ventana de edición de puerta (solapa "Identificación").

- **Dpto. de Entrada, Dpto. de Salida:** Cada puerta puede pertenecer a un Departamento (vea la [sección 4.4: Departamentos](#)) o limitar entre dos de ellos. Estos campos permiten ubicar a la puerta en la estructura de departamentos.
- **Lector de Entrada, Lector de Salida:** En estos campos se indica al sistema qué lectores (Lector #1 o Lector #2 del panel del que depende la puerta) serán utilizados y con qué función (Entrada o Salida).
- **Cámara de Entrada, Cámara de Salida:** Es posible asociar cámaras digitales para que capturen imágenes frente a eventos asociados a una puerta. Vea la [sección 5.1: Cámaras digitales asociadas a las puertas](#), para más información sobre este punto.

La figura 4.14.b muestra la segunda solapa de la ventana de edición de puertas (“Configuración”).

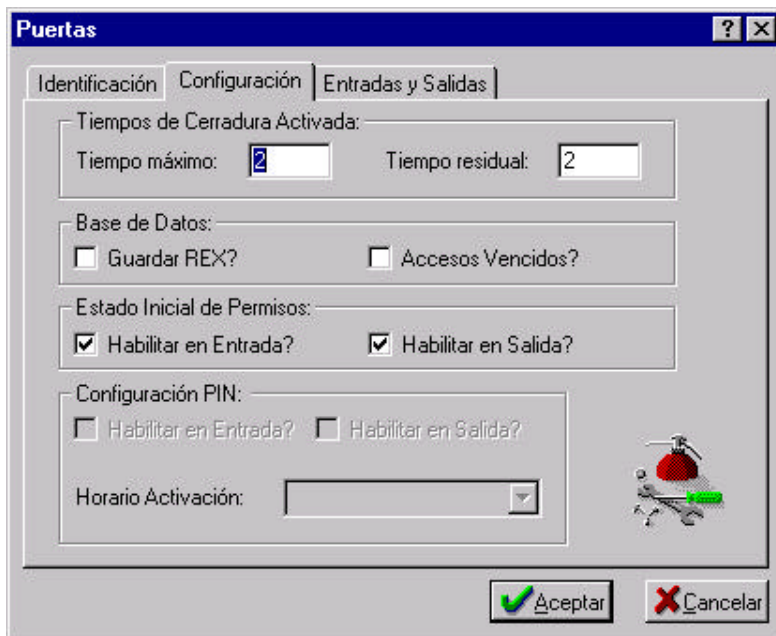


Figura 4.14.b. Ventana de edición de puerta (solapa “Configuración”).

Sus campos se describen a continuación:

- **Tiempo máximo:** Período de tiempo, expresado en segundos, durante el que el panel mantendrá abierta la cerradura de la puerta luego de dar la orden de apertura.
- **Tiempo residual:** Período de tiempo (en segundos) durante el que el panel mantendrá abierta la cerradura de la puerta a partir de la detección de la apertura real de la puerta (por medio del sensor de puerta abierta). Si no se especifica un tiempo residual, el panel sólo mantendrá abierta la cerradura por un período igual al tiempo máximo, a partir de la orden de apertura.

- **Guardar REX?:** Seleccione esta casilla si desea que las aperturas por REX (pulsador de salida) también se almacenen con los eventos en la base de datos.
- **Accesos Vencidos?:** Seleccione esta casilla si desea que los eventos producidos cuando el usuario no abre la puerta dentro del período de tiempo especificado en el campo **Tiempo máximo**, también se almacenen en la base de datos.

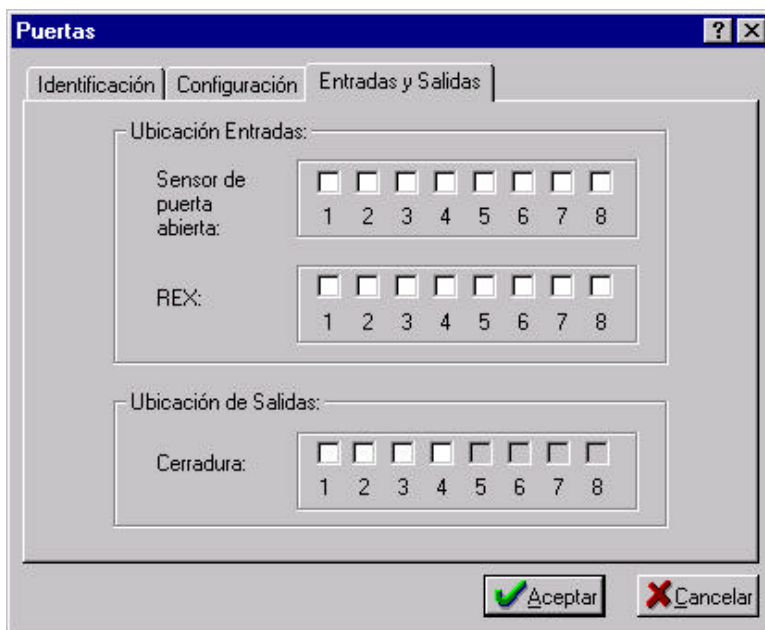


Figura 4.14.c. Ventana de edición de puerta (solapa “Entradas y Salidas”).

- **Estado inicial de Permisos - Habilitar en Entrada? / Habilitar en Salida?:** Si estas casillas están seleccionadas, los permisos de acceso que se den sobre la puerta serán habilitados ni bien el panel reciba la programación de los mismos. En sistemas donde se utilizan los desencadenadores del NeoLock, es posible que no se desee habilitar los permisos hasta que no se dispare un desencadenador. En este último caso, estas casillas no

deben estar seleccionadas. Si usted no está utilizando desencadenadores, debe dejar seleccionadas estas opciones (opción por defecto). Para obtener más información sobre los desencadenadores, consulte la [sección 5.3: Desencadenadores](#).

- **Configuración PIN - Habilitar en Entrada? / Habilitar en Salida?:** Esta opción sólo está disponible en puertas que dependen de paneles cuyo modelo soporta lectores con PIN (clave ingresada por teclado para confirmar la identificación por tarjeta del usuario). Si posee paneles y lectores con esta función, puede habilitarla o deshabilitarla por software mediante esta opción.
- **Configuración PIN – Horario Activación:** Si el PIN está habilitado en la salida o en la entrada, debe definirse el horario en que el mismo estará activo. El mismo es un horario de NeoLock, cuya estructura se describe en la [sección 4.6.1: Bandas y Horarios](#).

La figura 4.14.c presenta la tercer solapa de la ventana de edición de puertas (“Entradas y Salidas”).

En ella hay 2 grupos de casillas de selección:

- **Ubicación de las Entradas:** Aquí se seleccionan las entradas del panel asociadas a esta puerta. Los datos ingresados en esta ventana deberán reflejar el conexionado físico del sensor de puerta abierta y del pulsador de salida (REX) con el panel. Nótese que una puerta puede no tener sensor de puerta abierta ni REX. Es posible, como se indicó en la [sección 4.3.2](#), que el sistema interprete estas entradas como normal cerradas o como normal abiertas.
- **Ubicación de las Salidas:** En estas casillas se indica la, o las salidas de relé del panel que se accionarán cuando el panel intente abrir la puerta. Para configurar una salida como normal abierta o como normal cerrada, debe modificar el jumper de la misma en el panel. Para más información sobre esta operación, consulte el Manual de Instalación del Hardware, Ref.: ADV_NK0003.

NOTA:

Al configurar las entradas y salidas de una puerta, debe tener el cuidado de no “solaparlas” con las asociadas a la otra puerta del panel (si es que ésta existe). Del mismo modo, no debe seleccionar una misma entrada para el sensor de puerta abierta y para el REX.

4.3.4. Alarmas de puerta

Cuando el sistema detecta ciertas eventualidades, tales como el forzado de una puerta, etc., es posible configurarlo para que envíe un evento de alarma al servidor. Además, es posible accionar una salida del panel, lo que permite activar algún otro mecanismo de alerta.

Existen cuatro tipos de alarmas en el sistema, asociadas a puertas. Éstas son:

- **Violación de puerta:** Se dispara cuando el sistema detecta que una puerta fue abierta (ya que se activa el sensor de puerta abierta), pero el panel controlador no dio la orden de abrirla.
- **Persona no reconocida:** Se produce cuando una persona intenta identificarse mediante una tarjeta que no está presente en la base de datos del panel controlador del que depende la puerta.
- **Persona fuera de horario:** Se activa al identificarse una persona en el lector de la puerta, fuera del horario en el que tiene permiso de acceso por la misma.
- **Puerta abierta:** Si una puerta fue abierta por el panel controlador, pero queda abierta más allá de un determinado tiempo (el cual es configurable), el sistema dispara esta alarma.

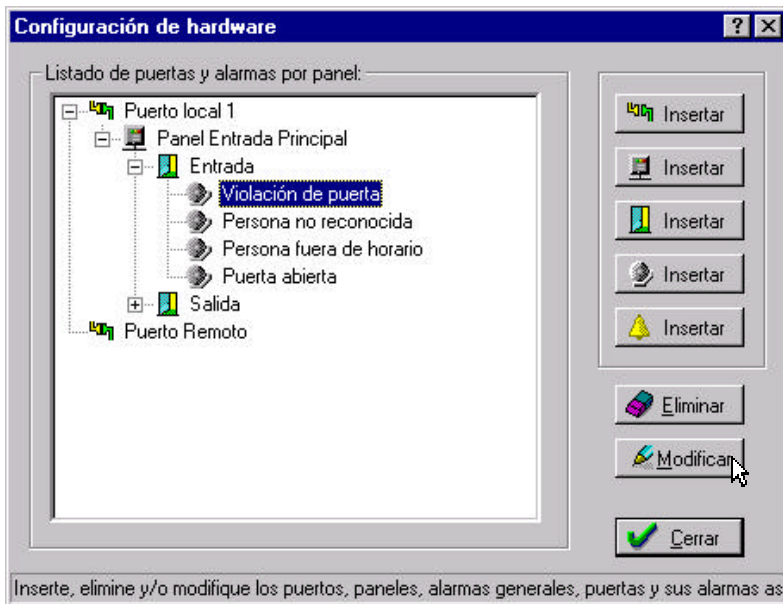


Figura 4.15. Modificación de una alarma de puerta.

Cuando es creada una puerta, el sistema agrega por defecto una alarma de cada tipo (4 en total).

Es posible modificar la configuración por defecto de cada una de ellas. Para esto, selecciónela con un click y presione el botón **Modificar** (figura 4.15). También puede eliminar alarmas que no desee y agregarlas luego (cuarto botón **Insertar** de la ventana de configuración del hardware).

Al presionar el botón **Modificar**, aparecerá la ventana de la figura 4.16.a. Sus campos son los siguientes:

- **Nombre:** Nombre que identificará a la alarma de puerta en el sistema. Puede contener hasta 30 caracteres.
- **Tipo:** Determina qué clase de alarma es. Puede ser uno de los cuatro tipos de alarma mencionados antes.
- **Horario de Activación:** Especifica en qué horarios estará activa la alarma. Fuera del horario aquí especificado, la

misma no se disparará. La estructura de los horarios de de NeoLock se ve en detalle en la [sección 4.6.1](#).

- **Horario Contrario?:** Mediante esta casilla de selección es posible negar el horario de activación de la alarma. Es especialmente útil para dejar funcionando las alarmas sólo en horarios donde no debe haber personas accediendo por la puerta.
- **Demora en verificación de alarma:** Tiempo, expresado en segundos, que debe mantenerse la condición de alarma para que sea reportada. Típicamente es cero, salvo para las alarmas de puerta abierta, a las cuales se las suele configurar para dispararse tras algunos segundos luego de la apertura.

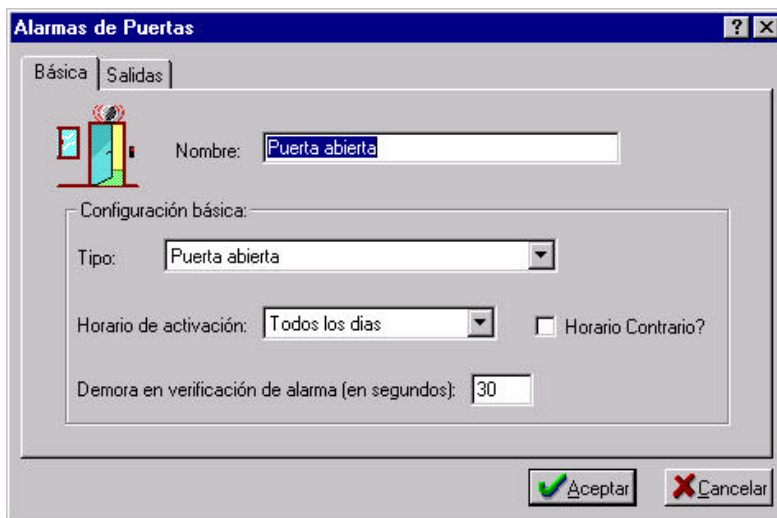


Figura 4.16.a. Ventana de edición de alarma de puerta (solapa “Básica”).

En la segunda solapa de la ventana de edición de alarma de puerta (figura 4.16.b) es posible asociar una salida física del panel para disparar algún mecanismo externo de alerta. Los campos de esta ventana son:

- **Ubicación:** Aquí se selecciona el número de la salida del panel que se activará frente a la alarma. Puede no seleccionarse ninguna. Nótese que una o dos de éstas salidas estarán ya destinadas a la/s cerradura/s de la/s puerta/s del panel.



Figura 4.16.b. Ventana de edición de alarma de puerta (solapa “Salidas”).

- **Modo:** Aquí se indica cómo será activada la salida asociada a la alarma (en caso de haber una). Sus posibles valores son “Señalización durante acontecimiento”, “Señalización ilimitada” y “Señalización por tiempo limitado”.
- **Cadencia:** La salida puede quedar activada (opción “Sin cadencia”) o funcionar intermitentemente (se dan varios períodos posibles para la intermitencia).
- **Duración de la señalización:** Si la opción seleccionada en **Modo**, es “Señalización por tiempo limitado”, aquí se especifica, en segundos, por cuánto tiempo estará activada la salida asociada a la alarma.

4.3.5. Alarmas generales

Además de las alarmas asociadas a las puertas, es posible también asociar alarmas a las entradas de sensor del panel controlador. Sensores de incendio, detectores de presencia, etc. pueden ser

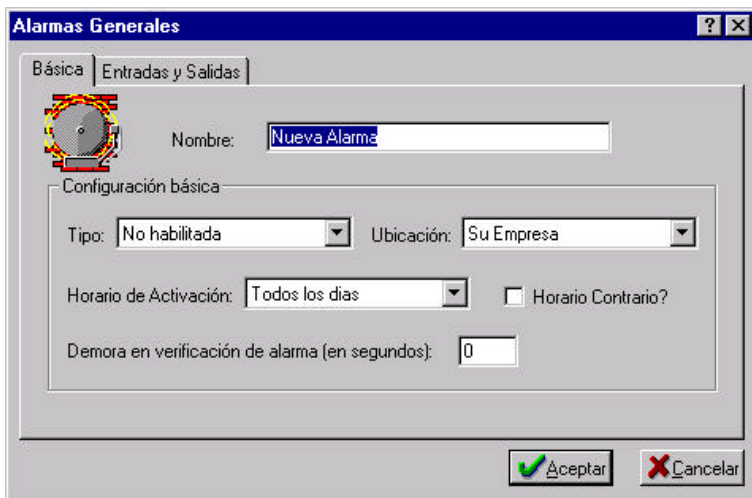


Figura 4.17.a. Ventana de edición de alarma general (solapa “Salidas”).

conectados a estas entradas. Este tipo de alarmas son llamadas en el sistema “Alarmas Generales”. Para agregar una, seleccione el panel deseado en la ventana de configuración del hardware y presione el quinto botón **Insertar**. Deberá aparecer en pantalla la ventana de la figura 4.17.a. Los campos de la misma son:

- **Nombre:** Nombre que identificará a la alarma general en el sistema. Puede contener hasta 30 caracteres.
- **Tipo:** Puede ser uno de 5 tipos:
 - **No habilitada:** la alarma no se disparará nunca.
 - **And de las entradas:** la alarma se disparará cuando todas las entradas seleccionadas se activen –ver la segunda solapa de la ventana-.
 - **Or de las entradas:** la alarma se disparará cuando una o más de las entradas seleccionadas se activen –ver la segunda solapa de la ventana-.

- **Temporizada:** la alarma se disparará durante el horario de activación seleccionado. Este tipo de alarmas se utilizan sobre todo para controlar indicadores (por ejemplo luminosos) que se activen durante determinados horarios.
- **Intrusión:** este tipo de alarma se utiliza en configuraciones donde un panel posee un lector de entrada y uno de salida para una única puerta de acceso a un recinto cerrado (de modo que la única forma de entrar o salir que un usuario tiene es pasando su tarjeta por el lector correspondiente). Básicamente, el panel contará la cantidad de usuarios adentro del recinto. Cuando la cuenta es mayor que cero (y por lo tanto hay alguien en el interior), la alarma permanece activa. Una vez que salió la última persona, la alarma se desactiva.
- **Ubicación:** Departamento al que pertenece la alarma (ver la [sección 4.4: Departamentos](#)).

Los campos **Horario de Activación**, **Horario Contrario** y **Demora en Verificación de Alarma** funcionan igual que los campos del mismo nombre descriptos en la [sección de alarmas de puerta](#).

Al igual que en las alarmas de puerta, es posible configurar la activación de una o más salidas del panel para accionar mecanismos de alerta externos. La configuración de las mismas es idéntica a la de las salidas asociadas a las alarmas de puerta. Sin embargo, en la segunda solapa de la ventana de edición de alarmas generales (figura 4.17.b) también hay una serie de casillas de selección llamadas Ubicación de las Entradas. En ellas es donde se seleccionan la o las entradas del panel controlador que dispararán la alarma.



Figura 4.17.b. Ventana de edición de alarma general (solapa “Entradas y Salidas”).

4.4. Departamentos

Para reflejar mejor la estructura de la instalación real del sistema de control de accesos, el NeoLock permite agrupar ciertos elementos (como las puertas o las alarmas generales) en “departamentos”. Además, cada departamento puede contener a su vez “subdepartamentos”.

Para editar los departamentos, haga click en el menú mostrado en la figura 4.18.

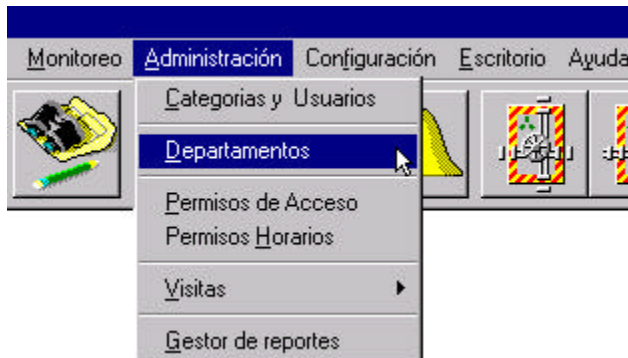


Figura 4.18. Menú Departamentos.

Verá en pantalla la ventana de la figura 4.19. En el sistema siempre existe al menos un departamento. El nombre por defecto del mismo es “Su empresa”. Para cambiarlo, selecciónelo con un click del mouse y presione el botón **Modificar**. Éste es el llamado *departamento base*.

Para insertar nuevos departamentos, presione el botón **Insertar**. Se desplegará una pequeña ventana que le permitirá editar el nombre (el cual puede contener hasta 20 caracteres). Si presiona el botón **Insertar** con un departamento seleccionado, el nuevo departamento será un subdepartamento del seleccionado. (Note que todos los departamentos son subdepartamentos del departamento base).

Siempre es posible borrar departamentos, para lo que debe presionar el botón **Eliminar**. El único que no puede ser eliminado es el departamento base. Si borra un departamento que contiene subdepartamentos, el sistema los eliminará automáticamente.

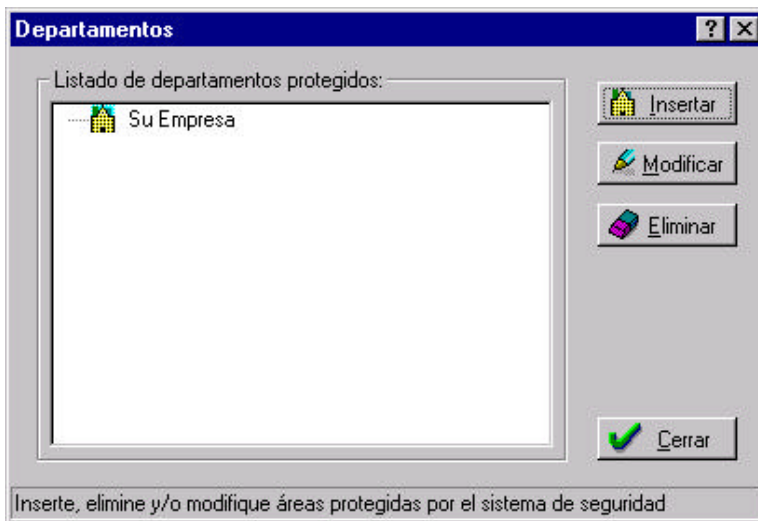


Figura 4.19. Ventana de edición de departamentos.

4.5. Categorías, Vehículos y Usuarios

Haciendo click en el menú de la figura 4.20, se abrirá la ventana de Categorías, Vehículos y Usuarios (figura 4.21).

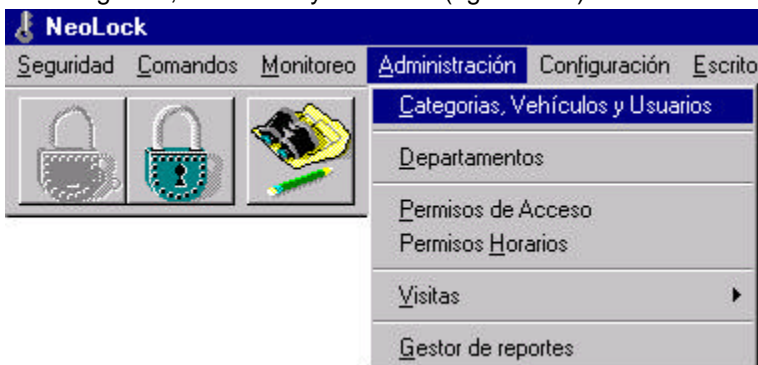


Figura 4.20. Menú de Categorías, Vehículos y Usuarios.

4.5.1. Categorías

Las categorías permiten organizar a los usuarios y los



Figura 4.21. Ventana Categorías, Vehículos y Usuarios.

vehículos, facilitando las tareas relacionadas con éstos (como asignar permisos de acceso, hacer reportes, etc.).

Si presiona el botón de **Insertar Categoría**, verá la ventana de la figura 4.22. En ella deberá ingresar el nombre y el tipo de la nueva categoría (el tipo podrá ser Personas o Vehículos).



Figura 4.22. Ventana de edición de Categorías.

Si desea modificar el nombre de una categoría existente, selecciónela y presione el botón **Modificar**. Note que el tipo de una categoría no puede cambiarse una vez que ésta fue creada.

4.5.2. Usuarios

Para insertar un usuario, seleccione una categoría cuyo tipo es "Personas", y presione el botón de **Insertar Usuario/Vehículo**. Se desplegará la ventana de la figura 4.23.a. En ella podrá insertar los datos del mismo. Tenga en cuenta que de la aleta de "Datos Personales" (que es la que se ve en la figura mencionada), sólo el nombre y el apellido son campos obligatorios.

La figura 4.23.b muestra la aleta de "Datos del Sistema". A continuación se describen los campos de la misma:

- **Nro. Tarjeta:** Es el número de la tarjeta que el usuario utilizará para acceder al área controlada por el NeoLock. Los primeros 3 dígitos forman el "Facility Code", siendo los últimos 5 el número impreso en la parte externa de la tarjeta.

- **PIN:** Número de Identificación Personal (Personal Identification Number). Se utiliza en aquellos sistemas donde hay lectores con teclado para complementar a la tarjeta del usuario. Cuando no se utiliza, su valor debe ser cero.

Figura 4.23.a. Ventana de edición de Usuarios (aleta de Datos Personales).

- **Perfil:** El NeoLock tiene distintos niveles de acceso a los programas (independientes de los Permisos de Acceso). Cada usuario debe tener uno de los siguientes perfiles, lo cual determinará qué acciones le son permitidas:
 - **Administrador:** Los usuarios con este perfil pueden modificar cualquier dato de la configuración del NeoLock.
 - **Base de datos:** Este perfil está pensando para ser asignado a quienes podrán modificar los datos relativos a los usuarios, categorías, etc. (como números de tarjeta, datos personales, permisos de acceso, y otros), pero que no pueden alterar la configuración de hardware (Puertos, Paneles, Puertas y Alarmas).

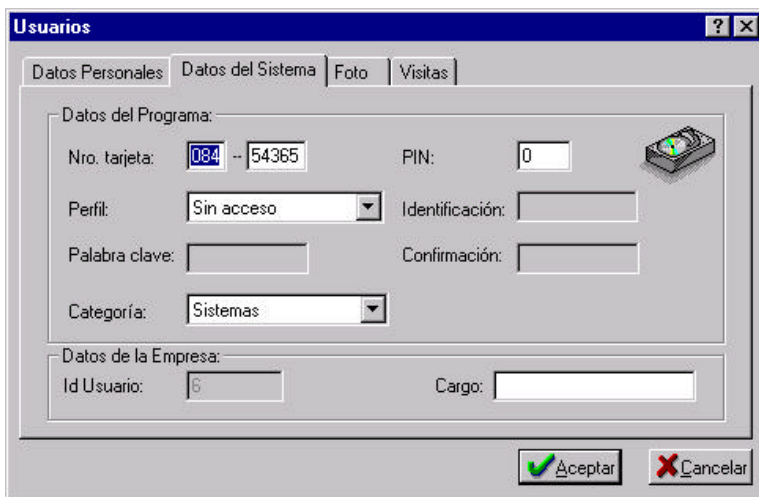


Figura 4.23.b. Ventana de edición de Usuarios (aleta de Datos del Sistema).

- **Configurador:** Permite alterar sólo la configuración de hardware (Paneles, Puertos, Puertas y Alarmas), sin modificar el resto de los datos del sistema.
- **Usuario:** Permite realizar sólo acciones de monitoreo, pero sin capacidad para modificar ningún dato del sistema. Es muy útil para guardias de seguridad, etc..
- **Sin acceso:** Los usuarios con este perfil no pueden entrar a los programas para realizar acción alguna. Sólo se les pueden asignar permisos de acceso por el área controlada.
- **Identificación:** En aquellos usuarios con perfil diferente de “Sin acceso”, la identificación es el nombre que el usuario escribirá al ingresar a los programas (en la ventana de la figura 4.2).
- **Palabra clave:** Además de la identificación, el usuario debe tener una palabra clave para ingresar al sistema. Es en este campo donde la especifica.

- **Confirmación:** Confirmación de la palabra clave, para evitar errores de tipeo que impidan el posterior ingreso al usuario.
- **Categoría:** Como se mencionó antes, cada usuario debe pertenecer a una categoría. Este campo permite cambiar al usuario de su categoría actual.
- **Id Usuario:** También llamado “Número de Legajo”. Es el número único que identifica al usuario. Una vez asignado no puede ser modificado. Como dos usuarios pueden tener el mismo nombre y apellido, éste es el verdadero identificador de usuario para el sistema.
- **Cargo:** Campo no obligatorio que permite especificar en el sistema del cargo del usuario..

Además de los datos mencionados, cada usuario puede tener una foto asociada. La misma puede provenir de un archivo (bmp o jpg) o puede ser capturada directamente con una cámara digital estándar (que el sistema operativo reconozca). La figura 4.23.c muestra la aleta de la foto del usuario.



Figura 4.23.c. Ventana de edición de Usuarios (aleta de Foto).

En la última aleta de la ventana de usuarios (figura 4.23.d), se puede asociar un usuario con el departamento donde trabaja, además de que es posible ingresar ciertos datos adicionales relacionados con el Módulo de Visitas de NeoLock. El funcionamiento en detalle de dicho módulo, así como el significado de los datos de esta aleta se explica en el manual del Módulo de Visitas (Ref.: ADV_NK0004).

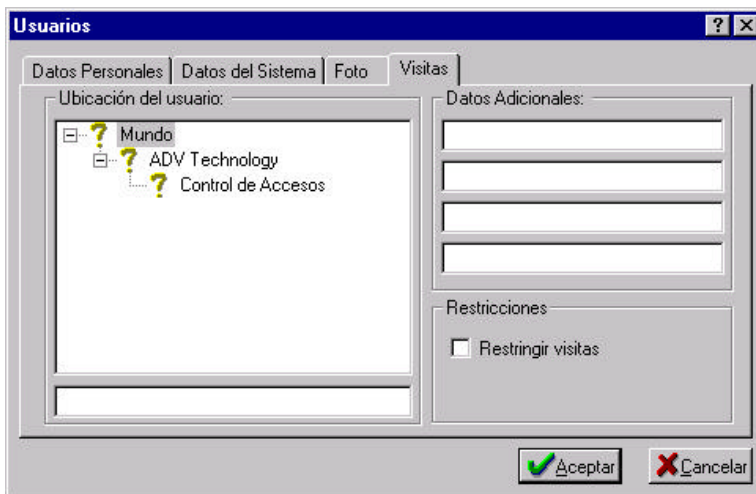


Figura 4.23.d. Ventana de edición de Usuarios (aleta de Visitas).

4.5.3. Vehículos

El NeoLock permite el control de accesos vehicular. Si selecciona una categoría cuyo tipo es "Vehículos", al presionar el botón **Insertar Usuario/Vehículo** verá la ventana de la figura 4.24.a. La misma es similar a la ventana de Usuarios. Los campos obligatorios son: **Marca, Modelo, Patente, Nombre (del Responsable) y Apellido (del Responsable)**.

Además, se puede especificar un remolque para cada vehículo. Los datos del remolque no son obligatorios y se ingresan en la ventana mostrada en la figura 4.24.b.

En cuanto a los datos del sistema, la ventana es exactamente igual a la de Datos del Sistema de Usuarios, sólo que un vehículo no tiene **Perfil, Identificación, Palabra Clave y Confirmación**.

Vehículos [?] [X]

Vehículo | Remolque | Datos del Sistema | Foto

Datos del Vehículo:

Marca: Modelo:

Color: Patente:

Nro Motor: Nro Chasis:

Tipo Vehículo: Cochera:

Datos del Responsable:

Nombre: Apellido:

Asignación: Teléfono:

Figura 4.24.a. Ventana de edición de Vehículos (aleta de Vehículo).

Por último, y al igual que los usuarios, también es posible asociar una foto al vehículo.

Vehículos [?] [X]

Vehículo | Remolque | Datos del Sistema | Foto

Datos del Remolque:

Marca: Modelo:

Color: Patente:

Nro Motor: Nro Chasis:




Figura 4.24.b. Ventana de edición de Vehículos (aleta de Remolque).

4.6. Permisos de acceso

Cada usuario o vehículo puede tener asignados permisos de acceso diferentes por cada puerta. Pero antes de asignar dichos permisos, es necesario definir los horarios en que éstos tendrán efecto.

4.6.1. Bandas y horarios

El menú de la figura 4.25 presentará en pantalla la ventana de Permisos Horarios (figura 4.26). En ella se pueden agregar nuevas



Figura 4.25. Menú de Permisos Horarios.

bandas además de las dos predefinidas por el sistema: “Nunca” y “Todo el día” (las cuales no pueden ser modificadas ni eliminadas). Al presionar el botón **Insertar**, se verá la ventana de la figura 4.27.

Una banda es un rango horario que puede tener como máximo 24 horas (00:00 hs. a 23:59 hs.) y que puede estar partida en dos segmentos, llamados en la ventana “Banda Horaria 1” y “Banda Horaria 2”.

Cuando se desea crear una banda que no esté dividida en segmentos, Banda Horaria 1 debe definirse exactamente igual a Banda Horaria 2. Por ejemplo, en la banda del sistema “Nunca”, Banda Horaria 1 y Banda Horaria 2 van de las 00:00 hs. a las 00:00 hs. En contraste, en la banda “Todo el día”, Banda Horaria 1 y Banda Horaria 2 van ambas de las 00:00 hs. a las 23:59 hs.. Una banda con salida al mediodía podría ser definida, por ejemplo, con Banda Horaria 1 desde las 08:00 hs. hasta las 12:00 hs. y con Banda Horaria 2 desde las 13:00 hasta las 16:00 hs..



Figura 4.26. Ventana de Permisos Horarios (aleta de Bandas Horarias).

Una vez que se han creado todas las bandas que se utilizarán, ya se puede definir un horario semanal.

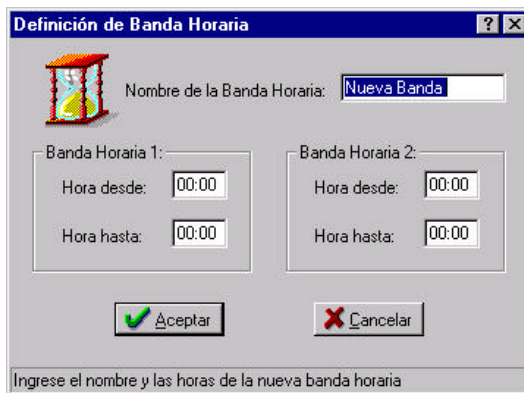


Figura 4.27. Ventana de Definición de Bandas Horarias.

La figura 4.28 presenta la aleta de Permisos Semanales. A cada uno de los días de la semana se puede asignar una banda (previamente creada), brindando una gran flexibilidad.

Definición de Horario Semanal

Nombre del Permiso Horario:

Horario Semanal:

Lunes	<input type="text" value="Nunca"/>	Martes	<input type="text" value="Nunca"/>
Miércoles	<input type="text" value="Nunca"/>	Jueves	<input type="text" value="Nunca"/>
Viernes	<input type="text" value="Nunca"/>	Sábado	<input type="text" value="Nunca"/>
Domingo	<input type="text" value="Nunca"/>	<input type="checkbox"/> Permiso Restringido	

Ingrese el nombre del nuevo permiso horario y la banda horaria para cada día de la semana

Figura 4.28. Ventana de Definición de Horario Semanal.

Existen como parte del sistema los permisos predefinidos “Nunca ” y “Todos los Días”. El primero tiene la banda “Nunca” asignada a los 7 días, mientras que el segundo tiene asignada a banda “Todo el día” también en los 7 días.

Por último, cabe mencionar a la casilla de selección **Permiso Restringido** (figura 4.28). Si la misma está seleccionada, la puerta sobre la que se asigne este permiso no se abrirá ni siquiera dentro del horario permitido. El sistema generará un evento de “Tarjeta Restringida”. Esta casilla debe utilizarse sólo si se tienen aplicaciones especiales desarrolladas a medida por ADV Technology S.R.L. que hacen uso de esta extensión.

4.6.2. Asignación de permisos de acceso

Una vez que un permiso horario ha sido definido, se lo puede asignar a un par usuario-puerta. Cada usuario puede tener permisos horarios diferentes en cada puerta. Para facilitar la tarea de asignación, también es posible dar un permiso por categoría y por departamento

(todos los usuarios de dicha categoría obtendrán así el permiso por todas las puertas del departamento en cuestión).

La figura 4.29 muestra la opción de menú que abre la ventana de Permisos de Acceso (figura 4.30).



Figura 4.29. Menú de Permisos de Acceso.

Hay dos formas de dar un permiso de acceso:

1. Puede seleccionar el usuario/categoría, seleccionar la puerta/departamento y luego presionar el botón de **Asignación** (en el centro de la ventana, con una flecha como ícono).
2. Puede seleccionar el usuario/categoría y arrastrarlo con el mouse hasta el departamento/puerta deseado.

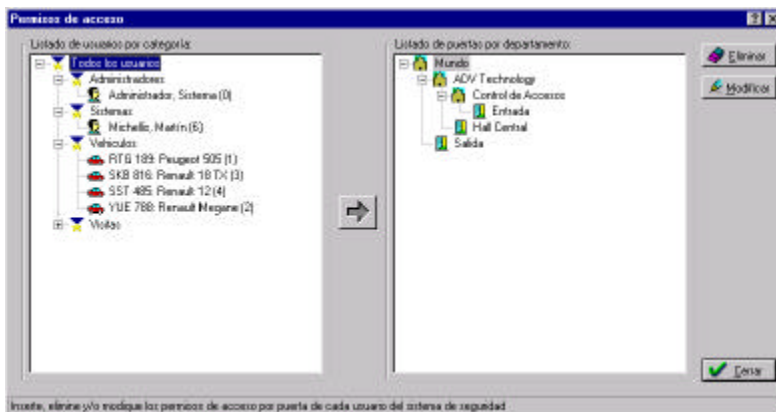


Figura 4.30. Ventana de Permisos de Acceso.

Al hacer esto, se desplegará la ventana de la figura 4.31, en la cual debe seleccionar el horario a asignar.

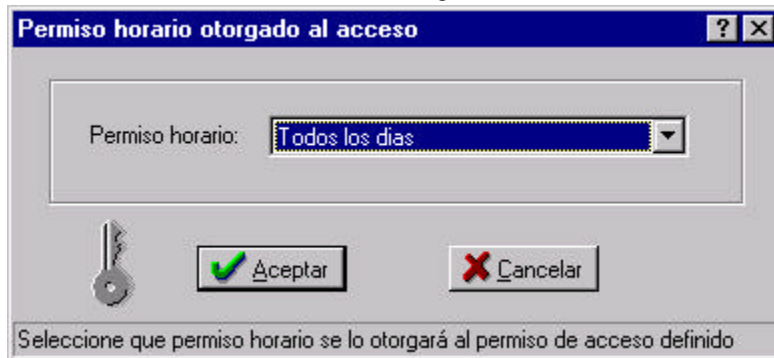


Figura 4.31. Ventana de Permiso horario otorgado al acceso.

1.7.4.7. Monitoreo

En la figura 4.32 se ve el menú **Monitoreo**. Con él se pueden ver las ventanas de Eventos On-Line e Identificación Visual, que se explican en las siguientes dos secciones.



Figura 4.32. Menú Monitoreo.

4.7.1. Eventos On-Line

La ventana de Eventos On-Line permite ver en tiempo real los eventos que se producen en el sistema. Haciendo click con el botón derecho del mouse sobre ella, es posible configurar qué columnas se ven, así como el orden con que las mismas aparecen en pantalla.

4.7.2. Identificación visual

La ventana de Identificación Visual (figura 4.33) permite ver la imagen capturada por la cámara asociada a la puerta, si la hubiere (ver [Sección 5.1. Cámaras digitales asociadas a las puertas](#)) junto a la imagen del usuario que figura en la base de datos. De esta forma es posible contrastar ambas para ver si se trata de la misma persona. Esto facilita la detección de irregularidades tales como el robo de tarjetas, etc..

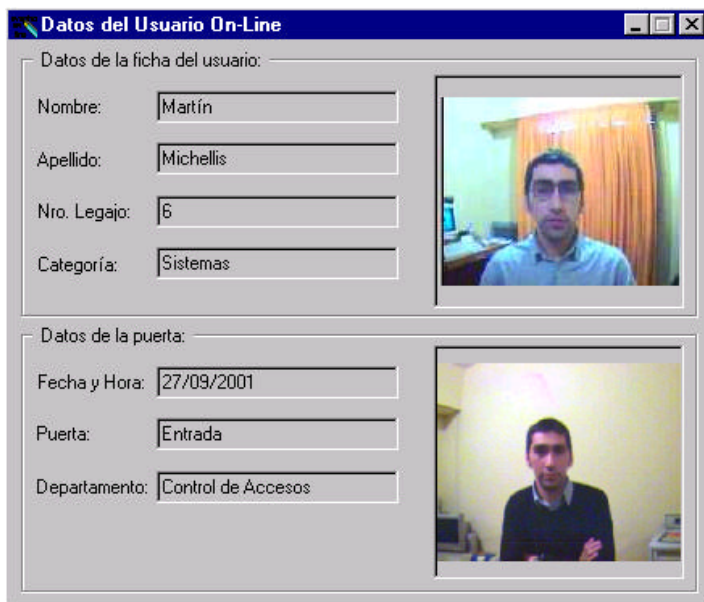


Figura 4.33. Ventana de Identificación Visual.

4.8. Comandos On-Line

Los Comandos On-Line permiten realizar acciones en tiempo real sobre los paneles controladores, sus puertas y alarmas.

A continuación se describen con más detalle.

4.8.1. Reconfiguración de los paneles

La ventana de reconfiguración de paneles (figura 4.34) permite sincronizar los datos de la base de la PC con la configuración real de los paneles. Para abrirla, seleccione el menú

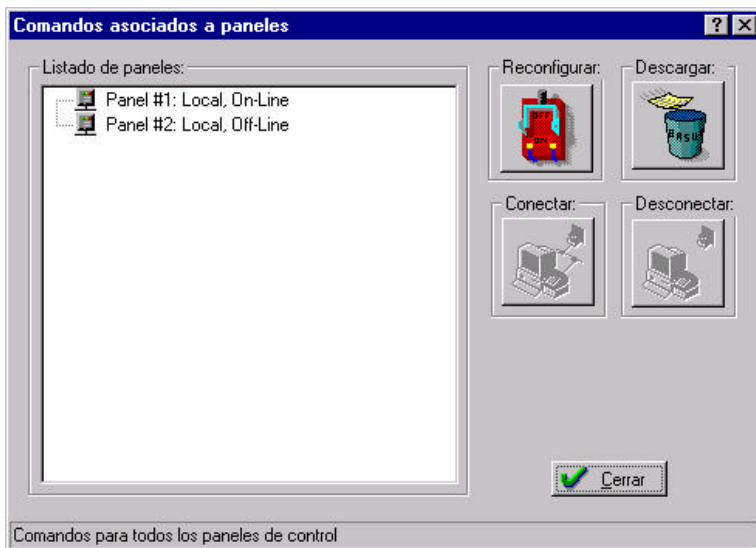


Figura 4.34. Ventana de Comandos asociados a Paneles.

Configuración:Comandos. En ella se puede seleccionar cualquier panel del sistema, sea éste local o remoto y enviarle su configuración de hardware (botón **Reconfigurar**) o vaciar su base de eventos (botón **Descargar**). En el caso de los paneles remotos, antes de reconfigurarlos/purgarlos, es necesario iniciar una conexión (botón **Conectar**) y terminarla al concluir las tareas (botón **Desconectar**).

4.8.2. Reprogramación de los relojes de los paneles

El menú **Configuración:Programar Relojes** resincroniza los relojes de todos los paneles del sistema con la fecha y hora de la PC.

4.8.3. Comandos de puertas y alarmas

La figura 4.36 muestra la ventana de Comandos para Puertas y sus Alarmas, la cual se abre al seleccionar el menú de la figura 4.35.

Los botones de esta ventana permiten abrir, bloquear y

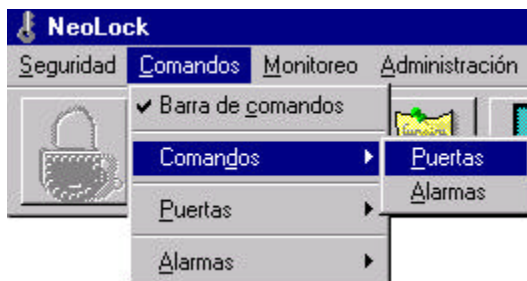


Figura 4.35. Menú Comandos.

normalizar puertas, así como apagar las alarmas de Puerta Abierta, Violación de Puerta, Tarjeta No Reconocida y Tarjeta Fuera de Horario (si están configuradas como “Señalización por tiempo ilimitado”, ver [sección 4.3.4](#)).

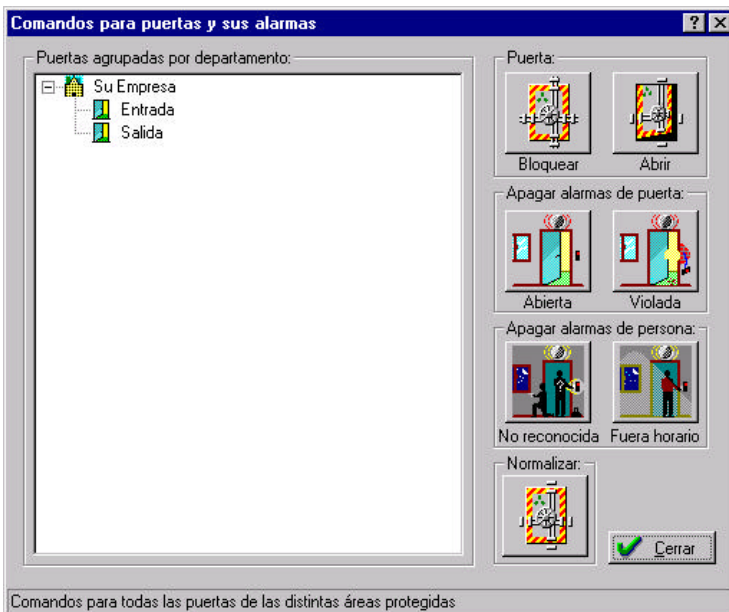


Figura 4.36. Ventana de Comandos de Puertas y Alarmas.

4.8.4. Comandos de alarmas generales

Las alarmas generales pueden ser disparadas, apagadas, bloqueadas o habilitadas mediante los botones de la ventana de Comandos Para las Alarmas Generales (figura 4.37).



Figura 4.37. Ventana de Comandos Para las Alarma Generales.

Para desplegar esta ventana, seleccione el menú **Comandos:Comandos: Alarmas** (figura 4.38).

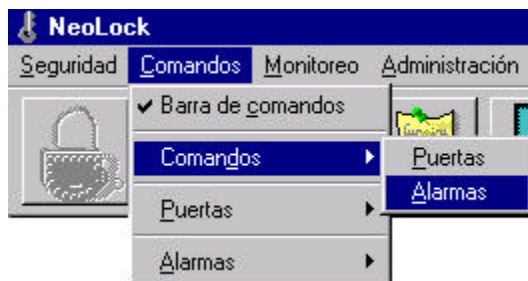


Figura 4.38. Menú de Comandos de Alarma Generales.

5. Funciones avanzadas

5.1. Cámaras digitales asociadas a las puertas

Cada puerta del sistema puede tener asociada una cámara digital TCP-IP para la captura de imágenes en tiempo real frente a un

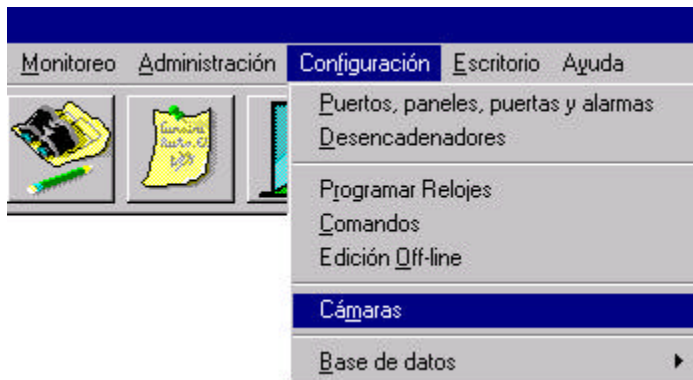


Figura 5. 1. Menú de Cámaras.

evento. Esto permite monitorear lo ocurrido en los accesos del área controlada, así como llevar registro de las imágenes. La figura 5.1 muestra el menú que abre la ventana de Cámaras (figura 5.2).

Al presionar el botón **Insertar**, se podrá ver la ventana de

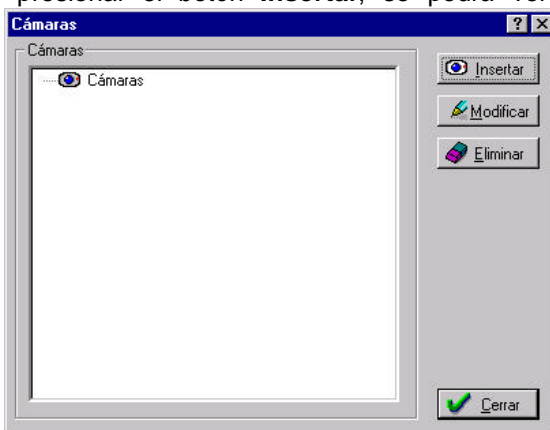


Figura 5.2. Ventana Cámaras.

Edición de la Cámara (figura 5.3). Cada cámara deberá tener un nombre único que la identifique en el sistema, y dos direcciones IP: una para la captura de fotos fijas y otra para la captura de video (generalmente, ambas direcciones son iguales). Los campos llamados **Comando** (tanto en el marco de Captura de Fotos como en el de **Captura de Video**) sólo deberían ser modificados por usuarios con conocimiento de la cámara que está siendo utilizada, ya que especifican el comando que el NeoLock enviará a la cámara para obtener las imágenes capturadas (el cual puede variar en los distintos tipos de cámaras existentes).

The image shows a Windows-style dialog box titled "Edición de la Cámara". It contains three main sections, each with a label and two input fields. The "Cámara" section has a "Nombre:" field with the text "Nueva Cámara". The "Video On-Line" section has a "Dirección:" field with "172.16.3.111" and a "Comando:" field with "/fullsize.jpg". The "Captura de Fotos" section has a "Dirección:" field with "172.16.3.111" and a "Comando:" field with "/fullsize.jpg". At the bottom right, there are two buttons: "Aceptar" with a green checkmark icon and "Cancelar" with a red X icon.

Figura 5.3. Ventana de Edición de Cámaras.

Una vez que se han dado de alta las cámaras del sistema, es posible asociarlas a una puerta. Esto se hace en la ventana de Edición de Puertas, en la solapa de Identificación. Vea la [Sección 4.3.3. Puertas](#) para obtener más información.

5.2. Búsqueda de personas en el área protegida

Para averiguar cuál fue el último acceso de una persona o vehículo (y de esta forma intentar ubicarlo dentro del área protegida), el NeoLock cuenta con un sistema de búsqueda.

Haciendo click en el menú **Seguridad:Buscar personas/vehículos** aparecerá la ventana mostrada en la figura 5.4.

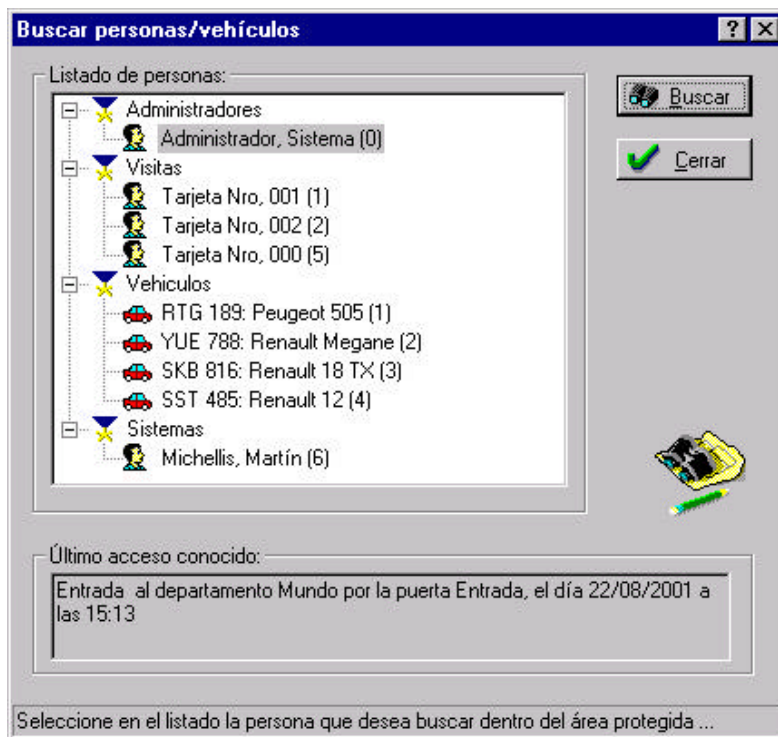


Figura 5.4. Ventana de búsqueda de personas/vehículos.

Al seleccionar una persona o un vehículo y presionar el botón **Buscar**, deberá aparecer en el cuadro de la parte inferior de la ventana el último acceso registrado correspondiente a esa persona o vehículo (si lo hubiere).

5.3. Desencadenadores y antipassback

El sistema de desencadenadores es el que hace posible la asignación dinámica de permisos en respuesta a eventos que ocurren en las puertas del área protegida. Haciendo click en el menú **Configuración:Desencadenadores** se desplegará la ventana de la figura 5.6, en la cual se listan todas las puertas, ordenadas por

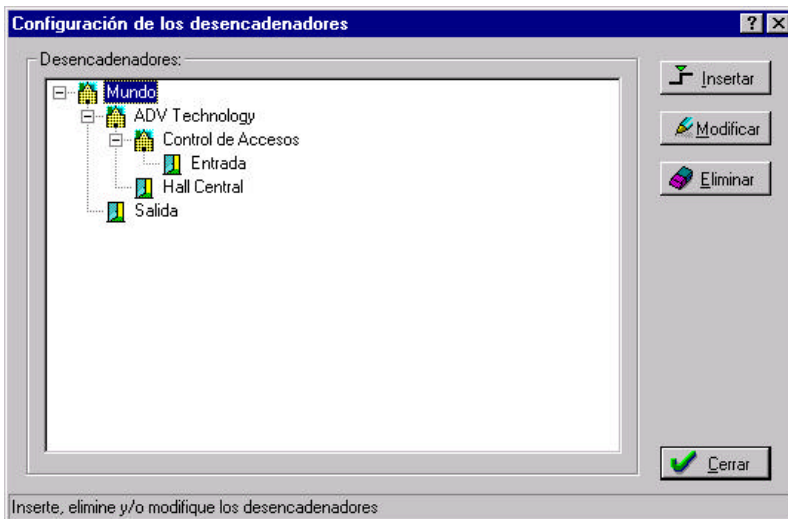


Figura 5.6. Ventana de Configuración de los Desencadenadores.

departamentos.

Un desencadenador es una acción que se disparará frente a un evento asociado a una puerta. Las acciones que puede realizar son habilitaciones/deshabilitaciones de permisos **sobre la tarjeta que generó la acción de disparo**. Esto implica que las acciones de otro usuario sobre la puerta no afectan más permisos que los de él mismo.

Para crear un nuevo desencadenador, seleccione una puerta de la lista y presione el botón **Insertar**. Verá la ventana de la figura 5.7.

Como se ve en la figura, deberá seleccionar la condición de disparo, que puede ser la entrada o la salida de un usuario (producida por la lectura de su tarjeta, ya que si la salida es por pulsador -REX-, no disparará el desencadenador por no poder determinar el usuario que realizó la acción).

Además de la acción de disparo, debe seleccionar la acción a tomar, y la puerta sobre la que la misma tendrá efecto. Si desea hacer más de una acción, deberá crear un nuevo desencadenador (en otras

palabras, habrá un desencadenador por par evento-acción). Las acciones posibles son la habilitación y la deshabilitación de **permisos existentes del usuario por la puerta sobre la que se actúa**. También es posible forzar un permiso que el usuario no tiene asignado por dicha puerta. Para esto, debe especificar el tipo **Forzar Entrada y Salida**, y seleccionar un permiso horario de la lista rotulada como **Horario** (la cual se habilitará automáticamente al seleccionar el tipo mencionado).

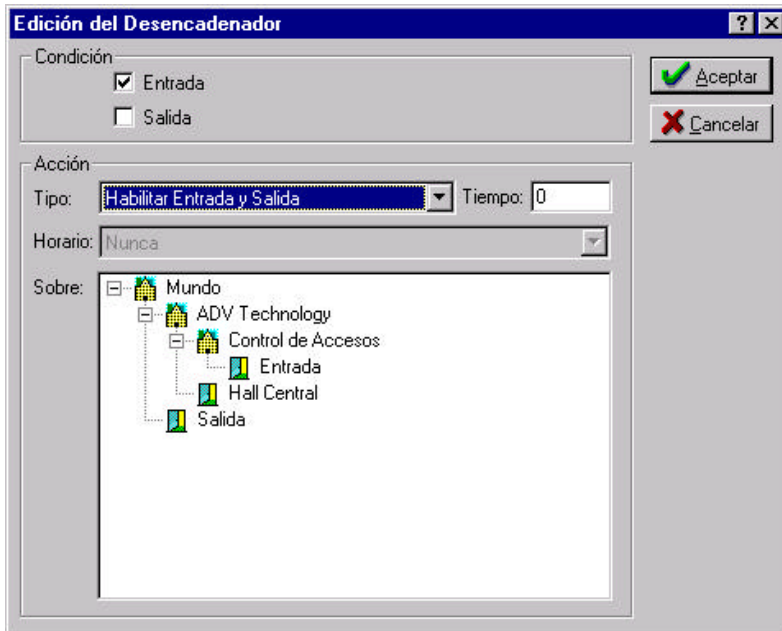


Figura 5.7. Ventana de Edición del Desencadenador.

Por último, es posible hacer que la acción tenga un tiempo de vencimiento (*time-out*). El mismo se ingresa en segundos, en la casilla denominada **Tiempo**.

6. Gestor de reportes

6.1. Funcionamiento general de los reportes

El NeoLock cuenta con un gestor de reportes que le permitirá consultar los datos del sistema, filtrándolos por diferentes criterios, y presentarlos en pantalla o en impresora. Además, posibilita la



Figura 6.1. Menú Gestor de reportes.

exportación de la información presentada al formato estándar DBF. La figura 6.1 muestra la entrada del menú para ejecutar el gestor de reportes. En la figura 6.2 puede verse la pantalla que se desplegará.

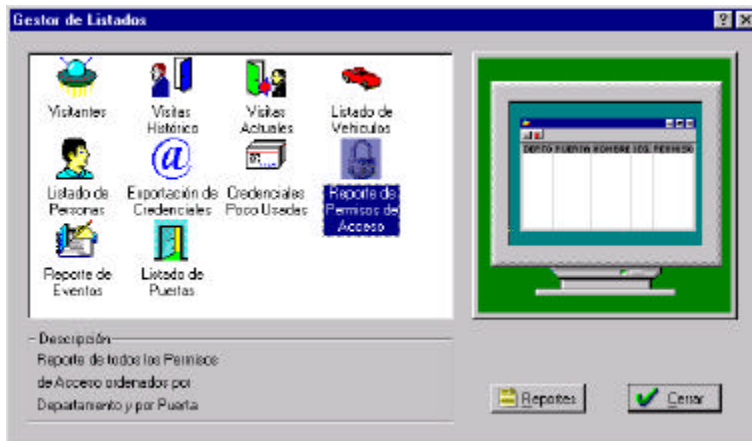


Figura 6.2. Ventana del gestor de reportes.

En ella puede seleccionar el ícono del reporte deseado y hacer doble click sobre él, o bien presionar el botón **Reportes**. A continuación, se describen los diferentes reportes con que cuenta el sistema.

6.2. Reporte de eventos

La figura 6.3 muestra la ventana de filtros del reporte de eventos. En ella se puede seleccionar la información a mostrar

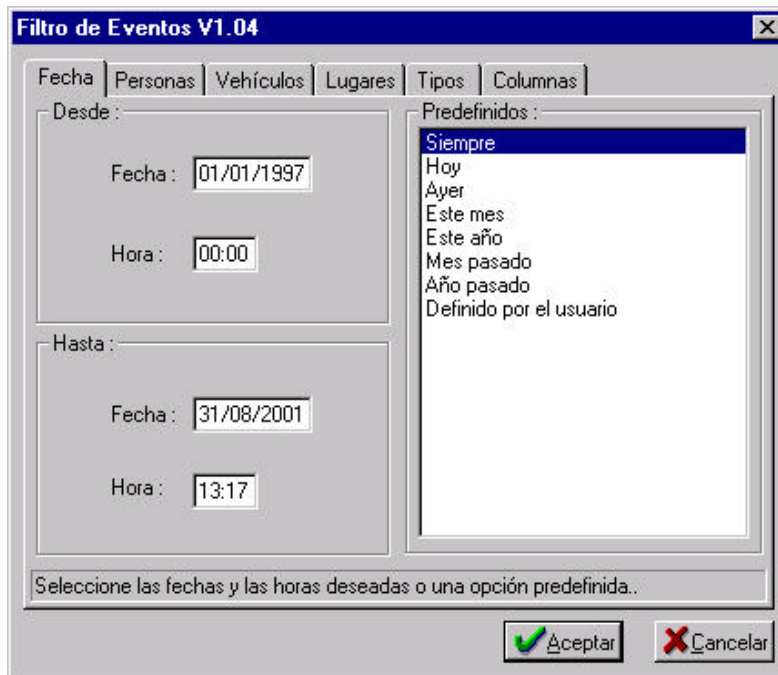


Figura 6.3. Ventana de filtros del reporte de eventos.

utilizando diferentes criterios. A cada criterio le corresponde una solapa de esta ventana. A continuación se da una breve explicación de cada aleta:

- **Fecha:** Sólo se mostrarán los eventos que se hayan producido dentro del rango de fechas seleccionado. Existen rangos predefinidos con los criterios más utilizados, como ser "Siempre", "Hoy", "Este mes", etc..

- **Personas** Si se filtra por personas, sólo se mostrarán los eventos asociados a ellas (sólo entradas y salidas, ya que las alarmas y otros eventos no corresponden a ninguna persona). También es posible filtrar por categoría. Para mostrar todos los eventos (y no sólo los asociados a personas), se deben seleccionar todas las categorías y todas las personas.
- **Vehículos:** Similar al filtro por “Personas”, pero para vehículos. Es posible filtrar tanto por número de patente como por modelo.
- **Lugares:** Permite seleccionar sólo aquellos eventos asociados a determinadas puertas y departamentos.
- **Tipos:** Sólo se mostrarán los eventos de los tipos seleccionados en este filtro.
- **Columnas:** Esta aleta no es un filtro, sino que permite al usuario decidir qué datos desea que el reporte presente y en qué orden.

Todos los reportes muestran una barra con botones para realizar determinadas acciones. La figura 6.4 muestra la barra correspondiente al reporte de eventos. Los botones de impresión,

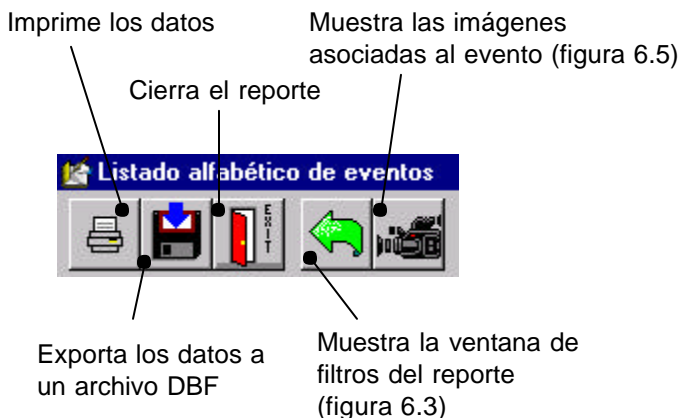


Figura 6.4. Barra de botones del reporte de eventos.

exportación a archivo DBF y cierre del reporte, son comunes a todos los reportes. Los demás son específicos del reporte de eventos. El botón para desplegar nuevamente la ventana de filtros aparecerá en todos aquellos reportes con filtros (algunos, como el reporte de puertas no poseen filtros). El botón para ver las imágenes asociadas al evento seleccionado desplegará la ventana de la figura 6.5. En ella se mostrará tanto la foto correspondiente al usuario asociado al evento (si lo hubiere), como la foto capturada en caso de que esté instalada una cámara digital en la puerta donde se produjo dicho evento.



Figura 6.5. Ventana de las imágenes asociadas al evento

6.3. Reporte de usuarios

El reporte de usuarios lista todos los usuarios del sistema, con

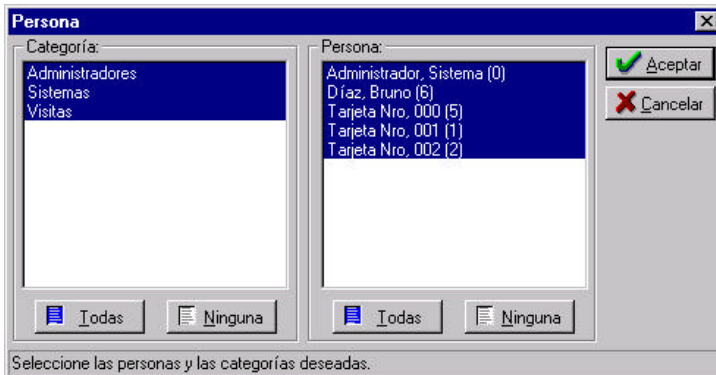


Figura 6.6. Ventana de filtros del reporte de usuarios.

sus datos asociados. La figura 6.6. muestra la ventana de filtros del mismo, que permite seleccionar tanto por usuario como por categoría (funciona del mismo modo que el filtro por personas del reporte de eventos.)

6.4. Reporte de permisos de acceso

Mediante este reporte se pueden listar todos los permisos de acceso otorgados a los distintos usuarios del sistema. La figura 6.7 muestra la ventana de filtros, en la cual se puede seleccionar el departamento al que corresponderán los permisos a mostrar.



Figura 6.7. Ventana de filtros del reporte de permisos de acceso.

6.5. Reporte de credenciales poco usadas

Este reporte permite listar aquellas credenciales que han tenido poco uso en el tiempo especificado.

Es especialmente útil a la hora de dar de baja tarjetas que no están siendo utilizadas. Sus aletas de filtro son:

- **Rango de Fechas:** Especifica el período de tiempo en el que se evaluará la cantidad de eventos de las credenciales.
- **Frecuencia de Uso de la Credencial:** Aquí se especifica cuántos eventos como máximo se tomarán para considerar a una credencial como poco usada (y así mostrarla en el listado).

6.6. Reporte de puertas

Mediante este reporte se listan todas las puertas del sistema, con el departamento al que corresponde cada una.

6.7. Reporte de vehículos

La figura 6.8 muestra la ventana de filtros del reporte de vehículos. Allí se puede seleccionar tanto por categoría como por vehículo. Su funcionamiento es similar al filtro por personas del reporte de eventos.

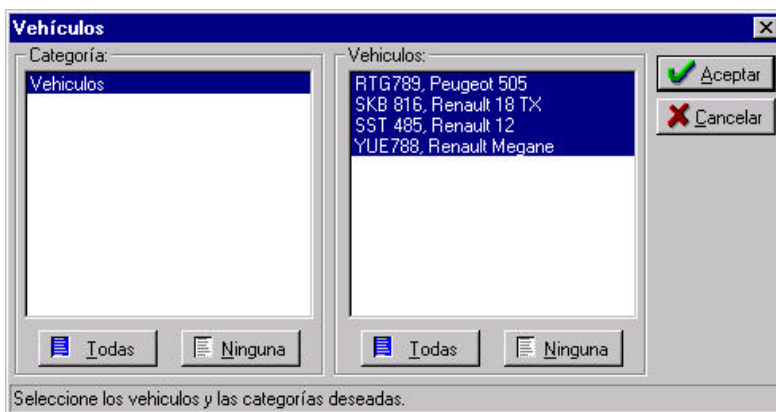


Figura 6.8. Ventana de filtros del reporte vehículos.

Apéndice A. Soporte técnico

ADV Technology S.R.L. le brinda a sus clientes el mejor producto posible. Hasta el momento de su impresión, la información de este manual totalmente actualizada. Para obtener la documentación de eventuales modificaciones y mejoras, puede consultar los archivos de documentación distribuidos en formato electrónico junto con el software, o visitar nuestro sitio web (www.advtechnology.com.ar).

Cuando usted se contacte con ADV Technology S.R.L., debe asegurarse de contar con la información que se incluye a continuación :

- Datos de la computadora: modelo, velocidad, capacidad libre del disco rígido y memoria con la que cuenta.
- Versión del Sistema Operativo (así como versión de eventuales “patches” / “service packs”) instalado.
- Número de serie de su producto (que se encuentra en la ventana “Acerca de...” del software).
- Tener escrito el texto de el/los mensaje/s de error exacto/s que se hayan producido.

A.1. Reemplazo de componentes

Para devolver algún componente del paquete NeoLock al Servicio Técnico Autorizado, usted debe contactarse con ADV Technology S.R.L. (la [contratapa](#) de este manual) o con un Distribuidor Autorizado para registrar su nombre, número de serie del producto, reclamo y número de factura de compra. Después de haber cumplido con este requisito, usted podrá devolver el componente a ADV Technology S.R.L. o al Distribuidor Autorizado. Cuando efectúe un reemplazo de componentes:

- Deberá incluir una fotocopia de la factura de compra, probando que el producto aún está bajo el período de garantía.

- El transporte, desde y hacia el Servicio Técnico Autorizado, así como también su costo, los daños, pérdidas o extravíos que se produzcan durante ese transporte, son responsabilidad del comprador.

La llave, los disquetes y/o documentación **reemplazados** pasarán a ser propiedad de ADV Technology S.R.L., quien garantiza que el producto reemplazado estará libre de defectos de materiales o mano de obra por un período de treinta (30) días desde la fecha de envío al comprador.

A.2. Solución de problemas y Manual para Instaladores

El manual ADV_NK0007, titulado “Manual para Instaladores” cuenta con una lista de posibles causas y soluciones para una serie de problemas que eventualmente puedan producirse en el sistema de control de accesos. Antes de recurrir a su distribuidor o a ADV Technology S.R.L., es recomendable consultar dicha documentación.

Apéndice B. Garantía

El paquete NeoLock está garantizado por ADV Technology S.R.L. contra defectos de manufactura en materiales, por un período de noventa (90) días. El mismo comienza el día de la fecha de compra que figura en la factura.

El reemplazo que la garantía cubre debe ser hecho en el Servicio Técnico Autorizado de ADV Technology S.R.L., según lo indica el Acuerdo Conjunto (ver el sobre que contiene los disquetes de instalación).

ADV Technology S.R.L. no se hace responsable por ninguna pérdida en las ganancias o daños comerciales, así como tampoco de daños incidentales, particulares u otros, que pudieran imputarse al uso de este producto.

B.1. Garantía del software

ADV Technology S.R.L. garantiza al comprador original que la llave de protección, los disquetes y la documentación incluida en este paquete, están libres de defectos por un período de noventa (90) días desde la fecha de compra que figura en la factura. En el caso de defectos en los materiales o mano de obra durante el período de garantía, ADV Technology S.R.L. reemplazará la llave de protección, el/los disquete/s o la documentación, cuando el producto defectuoso sea entregado a ADV Technology S.R.L. por el comprador. La garantía por este defecto está limitada a la reposición solamente, y no cubrirá otros daños como lucro cesante y/u otros reclamos incidentales, particulares o similares. Esta garantía no será aplicable y perderá su validez si el defecto es consecuencia de mal uso, maltrato o negligencia. ADV Technology S.R.L. no cubre otro tipo de garantías, ya sean orales o escritas, expresas o implícitas.

Antes de devolver el producto, contactarse con el Servicio Técnico Autorizado de ADV Technology S.R.L. (para el teléfono y dirección, ver la sección [A.1: Reemplazo de componentes](#)) o con un Distribuidor Autorizado, para registrar su nombre, número de serie del producto, reclamo y número de factura de compra. Después de haber cumplido con este requisito, usted podrá devolver el producto a ADV Technology S.R.L. o al Distribuidor Autorizado (junto a una fotocopia de la factura de compra). El transporte, desde y hacia el Servicio Técnico Autorizado, así como también su costo, los daños, pérdidas o extravíos

que se produzcan durante ese transporte, son responsabilidad del comprador. Si se determina que el producto es defectuoso, ADV Technology S.R.L. conviene en reemplazarlo o repararlo sin cargo, exceptuando los daños descritos anteriormente, siempre y cuando el producto sea acompañado de la factura original de compra.

La llave, los disquetes y/o documentación reemplazados pasarán a ser propiedad de ADV Technology S.R.L., quien garantiza que el producto reemplazado estará libre de defectos de materiales o mano de obra por un período de treinta (30) días desde la fecha de envío al comprador.

Notas:

Notas:

Notas: