

# DISEÑO E IMPLEMENTACIÓN DE UN SOFTWARE MEDIANTE VISUAL STUDIO PARA EL CONTROL DE ACCESOS CON EL NODO DE CONTROL INP-120F/V3 DE TECNOLOGÍA ESTÁNDAR LONWORKS

Sr. Ricardo Espín Brito  
Ing. Marcelo Escobar  
Ing. Jaime Andrango

Departamento de Eléctrica y Electrónica, Escuela Politécnica del Ejército  
Av. El Progreso S/N, Sangolquí, Ecuador

## 1. RESUMEN

*El presente proyecto presenta el diseño e implementación de un software para un sistema de control de accesos realizado mediante la herramienta de programación Visual Basic 6.0; este se lo realiza para la empresa ISDE - ECUADOR, que concibe la necesidad de complementar su sistema de control de accesos usando el nodo INP-120F/V3 de marca ISDE, que usa el protocolo abierto Lonworks; mediante un software, que le permita a un administrador sin conocimientos técnicos de este tipo de sistemas, controlar y monitorear el mismo.*

*El software es diseñado de acuerdo a las necesidades que un administrador y un determinado recinto requieren para un correcto control de accesos, incluyendo así una navegabilidad y operatividad amigable.*

*El software diseñado provee funciones como: monitoreo real de accesos válidos, dar de alta o de baja a un usuario, configuraciones básicas de los equipos de control de accesos; y una base de datos en la cual se pueden registrar usuarios, accesos válidos y alarmas que se producen en un sistema implementado.*

*Este software se lo implementa en la oficina de la empresa ISDE - ECUADOR para analizar y comprobar su funcionamiento, controlando así el ingreso y salida de los trabajadores.*

## 2. SOFTWARE DE CONTROL DE ACCESOS

El diseño de un software es una parte importante, en la implementación de un sistema de control y/o monitoreo, ya que este nos permite o permitirá conocer, usar y

evaluar de una forma más sencilla un sistema implementado.

En el diseño de un software, es importante manejar las necesidades y conocer los aspectos más relevantes de los usuarios que harán uso de dicho software, para poderles brindar las herramientas necesarias para el correcto de un determinado sistema.

### 2.1. Aspectos importantes previo diseño y programación

Antes de poder empezar a diseñar el software de accesos es importante conocer la configuración previa que tienen los nodos en la instalación del sistema de control de accesos.

Existe un software especializado para poder realizar la instalación y configuración inicial de los nodos de proximidad INP-120F de una manera técnica, este es LONMAKER; mediante el cual se puede conocer todas las variables existentes dentro de los nodos y/o configurarle para el propósito de la instalación.

Es importante este aspecto ya que con Lonmaker se crea una base de datos que representa el sistema donde se han implementado los nodos de control; dicha base de datos será de mucha ayuda, pues mediante el servidor LNSDDEServer y Visual Basic 6.0 se podrá crear una comunicación entre el PC y el nodo de proximidad que cumple las funciones configuradas en la base de datos, mediante el protocolo DDE.

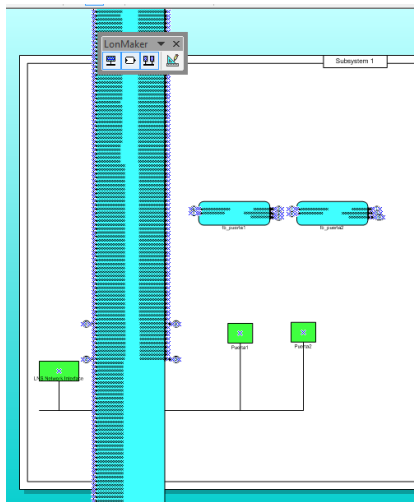


Figura. 2.1. Base de datos Lonmaker

En la figura. 2.1, se puede observar la base de datos mencionada, identificando brevemente a los nodos de control con cuadrados verdes y la interfaz de red USB con un rectángulo del mismo color. Además de los bloques funcionales de color celeste que contienen las variables de entrada y de salida de cada uno de ellos.

Regresando a la figura en cuestión, se observa que tenemos un bloque funcional con un sin número de variables de red, que corresponde a la interfaz de red USB; estas variables son creadas tomando el mismo tipo de variables existentes ya en los nodos de control, las variables creadas servirán para programar en el software de control de accesos.

Esto se lo realiza para que el software que se diseñe ataque a las variables directamente de la interfaz de red y no a las variables de cada uno de los nodos. Cabe indicar que las variables creadas se conectan a las variables de cada nodo de control (lógicamente), y esto se lo hace mediante el software Lonmaker.

A continuación se encuentra un ejemplo de lo expuesto:

```
Text9(0).LinkMode = 0
Text9(0).LinkTopic =
"LNSDDE|Tesis_3.Subsystem 1.DevNV"
Text9(0).LinkItem = "LNS Network
Interface.nvoEstCir2red.state
-t RAW"
Text9(0).LinkTimeout = 100
Text9(0).LinkMode = vbLinkAutomatic
```

- Conexión con LNSDDEServer, mediante el cual se conecta a la

base de datos creada en el software Lonmaker

```
"LNSDDE|Tesis_3.Subsystem 1.DevNV"
1 2 3
```

1. Servidor
2. Base de datos
3. Tipo de variable a escribir o leer

```
"LNS Network Interface.nvoEstCir2red.state
-t RAW"
1 2
```

1. Interfaz de red USB
2. Variable elegida del bloque funcional y formato del dato que se lee

Esto es un ejemplo para poder leer un dato, en este caso de la variable de salida *nvoEstCir2red*.

Para poder escribir primero se debe a tocar a una variable de salida como por ejemplo *nviSalida1*,

```
Text9(1).LinkMode = 0
Text9(1).LinkTopic =
"LNSDDE|Tesis_3.Subsystem 1.DevNV"
Text9(1).LinkItem = "LNS Network
Interface.nviSalida1red.state
-t RAW"
Text9(1).LinkTimeout = 100
Text9(1).LinkMode = vbLinkAutomatic
Text9(1).Text = "1"
Text9(1).LinkPoke
```

Como se observa el gran cambio es el tipo de variable que acepte escritura y el comando *Text9(1).LinkPoke*

## 2.2. Software de Control de accesos

Como se mencionó anteriormente el equipo a usar es el nodo de proximidad INP-120F, el cual permitirá controlar un solo acceso de un determinado recinto; es decir para cada acceso que se quiera controlar se debe añadir un nodo más.

El software a diseñar tiene como objeto; el ayudar y facilitar, al administrador de un recinto, el control y monitoreo del sistema de control de accesos implementado en el mismo. Mediante este software se podrá:

- Dar de alta o de baja a un usuario
- Poder deshabilitar o habilitar momentáneamente a un usuario.

- Controlar accesos válidos en tiempo real y mediante el registro en una base de datos.
- Controlar el número de usuarios que tienen acceso al recinto.
- Poder asignar un horario de entrada y de salida a determinados usuarios
- Controlar hasta un máximo de 50 accesos en el mismo recinto.

El software será diseñado mediante la herramienta de Visual Basic 6.0 que se la escogió con el objeto de disminuir costos; así que este pueda ser incluido como un extra y no como un gasto más dentro de sistema de control de accesos que se ofrece.

### 2.2.1. Diagrama de flujo

Para un mayor entendimiento del software que se desea diseñar se contempla el siguiente diagrama de flujo, en el cual se puede observar en una vista general lo que tendrá el software para el correcto y adecuado manejo del sistema de control de accesos.

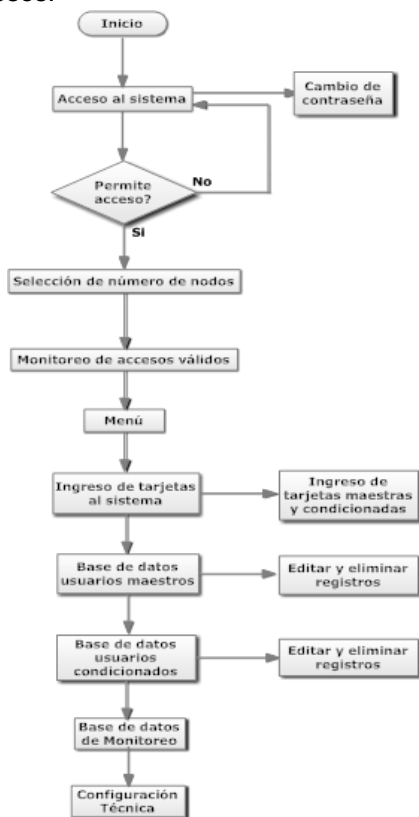


Figura. 2.2. Diagrama de flujo

## 2.3. DISEÑO DEL SOFTWARE

Considerando que el software a diseñar debe ser amigable, simple y de fácil uso para un usuario común que no tenga

conocimientos técnicos de los equipos de un sistema de control de accesos y que tenga conocimientos básicos de computación, se ha diseñado de la siguiente manera:

El diseño del software tendrá aspectos como son:

- Inicio del sistema
- Menú
- Ingreso de tarjetas:
  - o Tarjetas maestras
  - o Tarjetas condicionadas
- Base de datos:
  - o Usuarios maestros
  - o Usuarios condicionados
  - o Monitoreo de accesos válidos
- Monitoreo del sistema
- Configuración básica de equipos
- Alarmas: Puerta abierta y pérdida de comunicación

Para el diseño con estas características mencionadas, se realizarán las siguientes ventanas

### 2.3.1. Acceso Principal

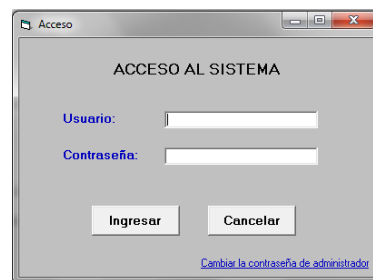


Figura. 2.3. Ventana de acceso al sistema

Esta ventana permitirá el acceso a un administrador o supervisor al software del sistema.

El administrador estará en capacidad de monitorear el sistema, como también dará de alta o de baja a las tarjetas de acceso al recinto. El **supervisor** tendrá el mismo acceso que el **administrador**, con la diferencia que este podrá cambiar su contraseña; y cambiar la contraseña del administrador si así se lo requiere por pérdida de la contraseña o por la necesidad de cambiarla.

Mediante una comparación de textos se podrá dar un acceso válido o no válido al software; la comparación se la realiza con una contraseña grabada tanto para el

administrador y el supervisor en la base de datos.

### 2.3.1.1. Tabla de datos contraseña

Para las contraseñas tanto para el administrador y el supervisor se crea una tabla en la base de datos "Registros" para almacenar las contraseñas que darán acceso al sistema.

### 2.3.2. Cambio de Contraseña

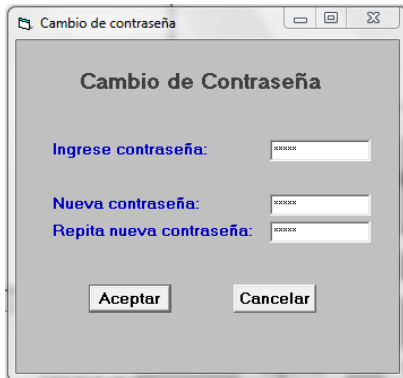


Figura. 2.4. Cambio de contraseña

Tal como se mencionó, se podrá cambiar la contraseña del administrador; esta acción podrá ser hecha solo por el supervisor. Esto se hace por medida de seguridad ya que si el administrador pierde la clave solo el supervisor (persona encargada de seguridad) tendrá el acceso al sistema y permitirá que el administrador pueda tener nuevamente acceso al software. Además el supervisor también será capaz de cambiar su propia contraseña.

Para dicho objetivo, el software consulta a la tabla correspondiente de la base de datos para poder extraer la contraseña que corresponde a cada usuario, y cambiarla si así se requiere. Se debe realizar lo siguiente:

1. Añadir un objeto ADODC, y un objeto del tipo datagrid para poder conectar con la tabla de contraseñas y poder así consultar los datos. Para este caso el objeto ADODC de llama **adodc1**. Para poder enlazarse con la tabla correspondiente es necesario seleccionar adodc1 en la propiedad DataSource del datagrid.
2. Para consultar los datos de la tabla Contraseña se usan comandos SQL.

Para el cambio de la contraseña, primero se debe elegir la contraseña que se quiere cambiar, en este caso para el Administrador o el Supervisor. Después se debe ingresar la contraseña del supervisor y proceder a poner la nueva contraseña dos veces en los campos correspondientes.

La Figura. 2.5 muestra, si se ingreso todos los datos correspondientes de la manera correcta.

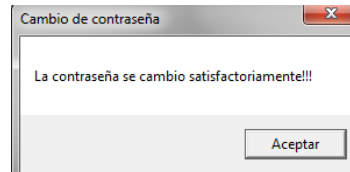


Figura. 2.5. Cambio de contraseña correcto

En el siguiente caso muestra si la contraseña del supervisor es incorrecta.

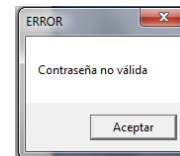


Figura. 2.6. Error contraseña

La siguiente figura muestra si la contraseña nueva no es igual en ambos campos donde se requiere escribirla.

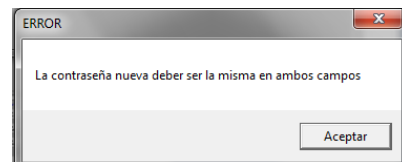


Figura. 2.7. Error nueva contraseña

### 2.3.3. Menú



Figura. 2.8. Menú

Esta ventana simplemente permite un acceso directo a cada una de las ventanas de las que consta el software que se explicarán a continuación, como se observa en la Figura. 2.9.

### 2.3.4. Selección de tarjetas



Figura. 2.9. Selección de Tarjetas

Esta ventana ayuda a seleccionar que tipo de tarjetas se requiere ingresar, habilitar o deshabilitar del sistema, ya sea maestra o condicionada.

#### 2.3.4.1. Ingreso de tarjetas maestras

El ingreso de tarjetas maestras es para usuarios que tienen un acceso con una sola limitante que es un horario por intervalos de días. Para el ingreso de este tipo de tarjetas se requieren los siguientes datos:



Figura. 2.10. Ingreso de Tarjetas Maestras

- Nombre del cliente al cual se le designa una determinada tarjeta.
- Número de casa al cual pertenece la persona a quien se le asigna una determinada tarjeta.
- El código de la tarjeta que se quiere configurar (previamente se debe pasar la tarjeta a programar por el lector de proximidad).

- Configuración del año, mes y día desde cuando la tarjeta podrá ser usada para un acceso válido.
- Configuración el año, mes y día hasta cuando la tarjeta podrá ser usada para un acceso válido.
- Selección a que puerta se le quiere dar acceso con la tarjeta.
- Posición de la lista propia del nodo de control de accesos en donde se guardará la configuración de una determinada tarjeta, permite el ingreso de 250 usuarios en este modo.

Lo que se hace en esta ventana es ingresar los datos requeridos en cada uno de los campos de un usuario, luego estos datos son ingresados al nodo transformándolos al tipo de dato que pueda ser aceptado por el nodo para la configuración, a través de la variable **nviDNIAdminitoMa**. Dichos datos se ingresan seleccionando **Ingresar a Dispositivo**.

Posteriormente, los datos también son ingresados a la tabla de datos de usuarios maestros; para ello también se debe añadir un objeto ADODC, que permita la conexión con la tabla Clientes.

En la ventana de ingreso de tarjetas maestras, también se puede seleccionar del buscador a que usuario se le quiere habilitar o deshabilitar. Al momento de seleccionar un usuario se cargan los valores de este usuario en los campos correspondientes y de esta manera se puede proceder a deshabilitar o habilitar al usuario según sea el caso.

Hay que tener en claro que para poder habilitar una tarjeta por este método, previamente se debe haber deshabilitado; de otra manera no tendría ningún objeto pues se sobreentiende que los usuarios existentes dentro de la base de datos tienen un acceso válido al recinto.

Al igual que cuando se deshabilita; para habilitar se escoge al usuario específico desde el buscador y se consultan los registros que este tiene en la base de datos, se los carga en la ventana de ingresos de tarjetas maestras y así se vuelve a cargar todos estos datos para poder habilitar al usuario.

### 2.3.4.2. Ingreso de tarjetas condicionadas

El ingreso de tarjetas condicionadas es para usuarios que tienen mayores limitantes en su horario, que son: intervalos de días e intervalos de horas/minutos entre días. Generalmente este tipo de tarjetas se les asigna a personas de la limpieza o mantenimiento que deben ingresar solo ciertos días y horas determinadas. Para el ingreso de este tipo de tarjetas se requieren los siguientes datos:




Figura. 2.11. Ingreso de Tarjetas Condicionadas

- Nombre del cliente al cual se le designa una determinada tarjeta.
- Número de casa al cual pertenece la persona a quien se le asigna una determinada tarjeta.
- El código de la tarjeta que se quiere configurar (previamente se debe pasar la tarjeta a programar por el lector de proximidad).
- Configuración el año, mes y día desde cuando la tarjeta podrá ser usada para un acceso válido.
- Configuración el año, mes y día hasta cuando la tarjeta podrá ser usada para un acceso válido.
- Configuración la hora y minuto desde cuando la tarjeta podrá ser usada para un acceso válido.
- Configuración la hora y minuto hasta cuando la tarjeta podrá ser usada para un acceso válido.
- Selección a que puerta se le quiere dar acceso con la tarjeta.
- Selección del tramo horario del día se quiere configurar, el equipo tiene hasta dos tramos horarios
- Selección del día de la semana en el cual se aplicará el horario elegido en los 4 puntos anteriores.

- Posición de la lista propia del nodo de control de accesos en donde se guardará la configuración de una determinada tarjeta, permite el ingreso de 50 usuarios en este modo.

Lo que se hace en esta ventana es ingresar los datos requeridos en cada uno de los campos de un usuario, luego estos datos son ingresados al nodo transformándolos al tipo de dato que pueda ser aceptado por el nodo para la configuración, a través de la variable **nviConfHoraria**. Se ingresan los datos seleccionando **Ingresar a Dispositivo**.

El ingreso de este tipo de tarjetas es similar para el ingreso de tarjetas maestras, a diferencia que sus datos son registrados en la tabla Clientescond de la base de datos; mediante la conexión que se realizará con un objeto ADO DC.

Esta ventana también permite buscar un usuario ya registrado en el sistema, pero para este caso en la tabla Clientescond; y poder deshabilitarle o habilitarle, según sea el caso.

### 2.3.5. Base de datos

Debido a ser un sistema de seguridad el control de accesos; es importante tener un registro de lo que sucede en el sistema, para lo cual es necesario registrar los usuarios habilitados en el sistema como también un monitoreo de los accesos que se producen en el recinto. Dicha base de datos se la realiza en Microsoft Office Access 2007, con el nombre Registro.

Se crearán cuatro tablas dentro de la base de datos, una tabla para usuarios maestros, una tabla para usuarios condicionados, una tabla para registrar accesos válidos y una tabla para registrar un evento de alarma. Cada una es independiente.

#### 2.3.5.1. Tabla de datos de usuarios maestros

Esta tabla de datos será para usuarios que tenga un acceso ilimitado diario al recinto dentro de un intervalo de tiempo, como por ejemplo: del 1 de Enero del 2011 al 1 de Enero del 2012.

Para ello se diseña la siguiente la tabla llamada Clientes que tendrá los campos

ingresados en la ventana de “Ingreso de tarjetas maestras”

Para poder acceder a la base de datos Registro desde Visual Basic 6.0, se sigue el mismo procedimiento para la tabla de las contraseñas:

Añadir un control ADODC y un objeto del tipo datagrid para poder conectar con la tabla y poder así consultar los datos.

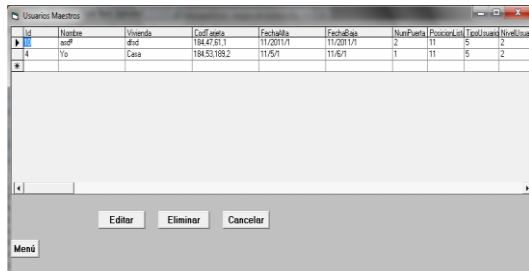


Figura. 2.12. Ventana tabla de datos de usuarios maestros

En esta ventana se han consultado los datos de la tabla Clientes, en esta ventana se brinda de opciones de **Eliminar** y **Editar** la información presente en la tabla.

### 2.3.5.2. Tabla de datos de usuarios condicionados

Esta tabla de datos será para usuarios que tenga un acceso limitado diario al recinto dentro de un intervalo de tiempo pero en determinado día y horario, como por ejemplo: del 1 de Enero del 2011 al 1 de Enero del 2012, solo los miércoles de de 7 a 9 am.

Para ello se diseña la tabla llamada Clientescond que tendrá los campos ingresados en la ventana “Ingreso de tarjetas condicionadas”

Para poder acceder a la base de datos Registro desde Visual Basic 6.0, se da el mismo procedimiento que para la tabla de datos de usuarios maestros, con la diferencia que para esta nueva ventana se debe añadir un nuevo objeto ADODC, que como se trata de una nueva ventana toma el nombre de adodc1; y un nuevo objeto datagrid para enlazar con la tabla.

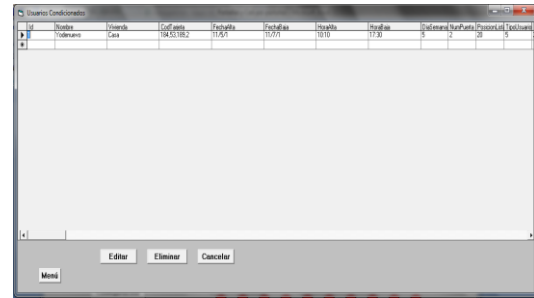


Figura. 2.13. Ventana de tabla de datos de usuarios condicionados

Al igual que en la tabla anterior, se tiene la opción de **eliminar** y **editar** la información que contiene la tabla.

### 2.3.5.3. Tabla de datos de monitoreo

Esta tabla ayuda a registrar cada uno de los accesos válidos al recinto que se han realizado por alguna puerta del recinto.

En esta tabla al igual que en las dos anteriores se deberá consultar los datos desde la base de datos, y de la misma manera añadir un objeto ADODC para el efecto, que como es otra nueva ventana toma el nombre de adodc1; y no olvidar añadir un objeto datagrid también.

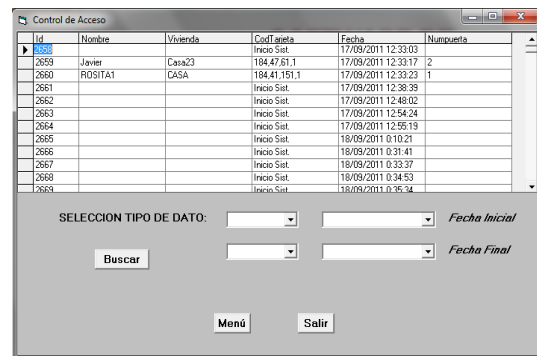


Figura. 2.14. Ventana de tabla de datos de control de acceso

Esta ventana sirve poder escoger o filtrar ciertos datos de la tabla de monitoreo de acuerdo al nombre, vivienda o fecha; mediante los campos mostrados en la figura. 2.18.

### 2.3.5.4. Tabla de datos filtro

Esta tabla se crea con el objeto de ingresar los datos que se han filtrado de la tabla de Acceso, a esta tabla se tiene acceso desde la ventana de base de datos de monitoreo.

Id	Nombre	Vivienda	Codf. Acceso	Fecha	Numpuerta
6666	Javier	Casa23	184.47.81.1	18/09/2011 1:29:21	2
6667	RIDISITA1	CASA	184.41.151.1	18/09/2011 1:30:00	1
6668	Javier	Casa23	184.47.81.1	18/09/2011 1:30:09	2
6669			Inicio Sist.	18/09/2011 1:30:32	
6670			Inicio Sist.	18/09/2011 1:31:13	
6671			Inicio Sist.	18/09/2011 1:31:25	
6672			Inicio Sist.	18/09/2011 1:32:46	
6673			Inicio Sist.	18/09/2011 1:32:55	
6674			Inicio Sist.	18/09/2011 1:33:07	
6675			Inicio Sist.	18/09/2011 1:35:57	
6676	Fady	Casa	184.47.81.1	18/09/2011 1:36:15	1
6677	Ricardo	Casa	184.41.151.1	18/09/2011 1:36:24	1
6678			Inicio Sist.	18/09/2011 1:43:57	
6679			Inicio Sist.	18/09/2011 1:31:07	

Figura. 2.15. Ventana de tabla de datos de filtro de accesos

Esta ventana permite tener una vista de los datos filtrados de la tabla de datos Acceso, además de ello permite exportar esta tabla a un hoja de Excel; desde la cual se podrá imprimir si se lo desea. Para la programación de esta exportación no olvidar activar **Microsoft Excel 12.0 Object Library**

### 2.3.5.5. Base de datos de alarmas

Esta tabla ayuda a registrar cuando alguna puerta del recinto se ha quedado abierta más de un determinado tiempo previamente configurado en el nodo de control.

Esta alarma se produce en la pantalla de monitoreo justo el momento que se detecta una alarma de puerta abierta en cualquier de los accesos del recinto, como se puede observar en la figura. 2.22.

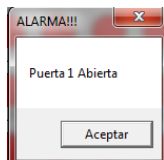


Figura. 2.16. Ventana de aviso de alarmas

### 2.3.6. Monitoreo

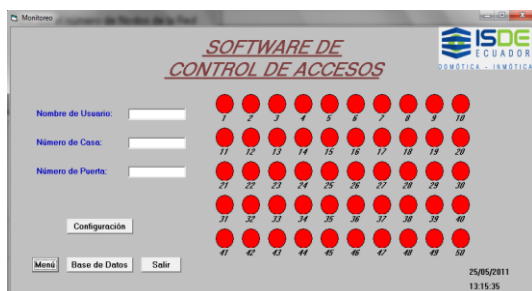


Figura. 2.17. Monitoreo del sistema

En la ventana de monitoreo del sistema se hará un monitoreo continuo de cada uno de los accesos del recinto, comunicándose cada uno de los nodos al software mediante el protocolo DDE. El monitoreo se realizará comunicándose con la variable de salida **nvoEstCir2red** que informa de estado de la cerradura electromagnética de cada uno de los nodos instalados. Esto se realizará mediante textos auxiliares que permitirán captar el estado de la variable en cuestión. Algo importante que se debe recordar es que cada uno de los estados de la salida de cada nodo deben ser guardados en diferentes textos para después diferenciar cada uno de ellos.

En la ventana se pueden observar dos partes, la parte izquierda que son los campos en los cuales se mostrará información de los usuarios que han ingresado al recinto, y en la parte derecha se podrá observar el acceso específico por el cual lo han hecho. Además consta de una tercera parte pero de ingresos directos a **Tabla de datos** de monitoreo, **Configuración** (configuraciones básicas de los equipos) y **Menú**.

Con la detección del estado de los accesos del recinto, en el monitoreo es necesario identificar que usuario y con qué número de tarjeta ha realizado un acceso válido al recinto. Para ello se debe comunicar con la variable de salida **nvoDatosLeidosV**, la cual devuelve los datos de la tarjeta que está siendo usada.

El valor que devuelve este variable es una serie de números que identifican a la tarjeta que se ha acercado al lector de proximidad, tales como: 0,0,191,183,145,1,0,1,7,216,1,23,12,18,56,7,19. Siendo los datos en negrilla los códigos de la tarjeta que van a interesar.

Identificado el estado del acceso y captado el código de la tarjeta, se procede a analizar si se produjo o no un acceso válido en el recinto, para lo cual si se dio un acceso válido este estado será detectado por el software y junto al código de la tarjeta se accederá a la tabla de datos del tipo de usuario que accedió; ya sea este maestro o condicionado. De esta manera se podrá identificar al usuario que ingreso al recinto y poder registrarlo en la base de datos de monitoreo.

En este caso se tiene acceso a las tres tablas de la base de datos, tanto a la Cliente,



Clientescond y Accesos. Para ello se deben añadir tres objetos ADODC, por cada una de las tablas. Tomarán los nombres de adodc1, adodc2 y adodc3. Además se deberá añadir tres objetos datagrid para cada uno de los objetos ADODC y los comandos SQL necesarios.

Algo importante en el monitoreo es el manejo de alarmas, para el caso se contempla un evento de puerta abierta, el cual hace que se produzca una alarma cuando una puerta no se ha cerrado y ya ha pasado el tiempo necesario para que un usuario acceda a una puerta del recinto.

Para lograr detectar la alarma de debe atacar a la variable **nviAlrPuerta**, que indica si ya ha pasado un tiempo determinado para que se dé la alarma. Ocurrida la alarma se enlaza con la base de datos a través de un objeto ADODC que toma el nombre de adodc4, el objeto de datagrid y el comando SQL necesario.

### 2.3.7. Acceso técnico

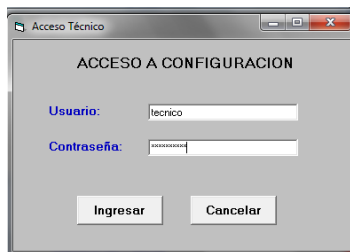


Figura. 2.18. Ingreso a Configuración

Este acceso solo será permitido a un técnico especializado en el sistema de control de accesos, con un usuario y contraseña diferente al acceso principal.

### 2.3.8. Configuración técnica



Figura. 2.19. Configuración

A esta ventana solo tendrá acceso un técnico especializado, que podrá realizar configuraciones básicas de los nodos, como son tiempo de apertura, fecha y hora.

También se contempló poder manejar manualmente las dos salidas que contiene el nodo si se lo requiere en algún momento; activarlas o desactivarlas.

Para realizar la lectura o modificación de la configuración de algún nodo en específico, se selecciona dicho nodo en la pestaña **Número de Puerta**; con ello realizado se ataca a las variables **UCP\_Type\_4[1]** y **nviFecha**; con las cuales de podrá cambiar el tiempo de apertura de la cerradura y la fecha del nodo, respectivamente.

### 2.3.9. Control de Comunicación

Se ha tomado en cuenta mensajes de error de comunicación, el cual permitirá que al iniciarse el software se pueda comprobar la buena comunicación con todos los nodos de control de accesos.

Para ello, se lee una variable cualquiera del nodo de control para comprobar su comunicación, si la comunicación es correcta no saldrá ningún mensaje; pero si ocurre un error saldrá un mensaje indicando el nodo en el cual falló la comunicación.

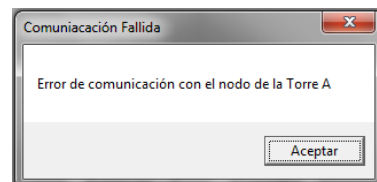


Figura. 2.20. Mensaje de error de comunicación

Al inicio del sistema mientras el PC lee todas las variables del nodo tiene un retardo considerable para lo cual se prevé una ventana de carga de información, como la que se muestra en la figura. 2.27.

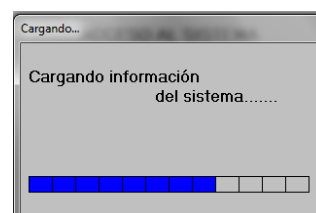


Figura. 2.21. Mensaje de error de comunicación

### 3. CONCLUSIONES Y RECOMENDACIONES

#### 3.1. Conclusiones

- Se ha realizado un software de control de accesos mediante Visual Basic 6.0 para programar y controlar desde una PC una red Lonworks que contenga hasta 50 nodos de proximidad INP-120/F.
- El software diseñado es amigable y fácil de usar, el cual permite que un administrador sin conocimientos avanzados de los equipos del sistema de control de accesos, pueda monitorear y controlar el sistema sin ningún inconveniente o ayuda de un técnico especializado.
- Se reducen los gastos operativos, que son necesarios para el sistema como son: dar de alta o de baja tarjetas de proximidad, configuraciones básicas de los equipos como fecha/hora y tiempo de activación de cerradura. Todos estos procedimientos no tendrán que ser contratados como extras pues con el software el mismo administrador del recinto podrá hacerlos tranquilamente desde el computador.
- Se crea un software capaz de programar totalmente un nodo de proximidad INP-120/F, que permite controlar y monitorear los accesos de un determinado recinto; mediante una base de datos que informa de cada uno de los accesos válidos que se producen y alarmas de puerta abierta que se pueden producir; dando así un nivel de seguridad importante al sistema de control de accesos.
- Mediante la instalación del software en las oficinas de ISDE – ECUADOR, el control de los trabajadores aumenta en gran medida, así como la seguridad pues se tiene una base de datos detallada de todos los accesos que se producen en la oficina, como también una base de datos de los usuarios que tienen acceso.

#### 3.2. Recomendaciones

- La tecnología Lonworks, además del uso del protocolo DDE para el control y monitoreo de sus redes, también tiene la posibilidad de usar el protocolo OPC (Control de procesos OLE). Por ello se recomienda un estudio profundo del mismo, ya que para instalaciones más grandes donde el número de equipos y sistemas aumenta se necesitará un protocolo más robusto donde se permita mayor capacidad de transmisión de datos, y no solo con un cliente, sino con varios lo cual el protocolo DDE no permite.
- Para un sistema de control de accesos es importante tomar en cuenta, el nivel de seguridad que se necesita, es así que si se quiere una mayor seguridad se recomienda realizar cambios en hardware con el uso de teclados o lectores de huellas dactilares, siempre y cuando estos cumplan con el protocolo Wiegand 26 para el correcto acople con el nodo de proximidad INP-120/F.

### 4. BIBLIOGRAFIA

- CALAFAT, Cristhian, **Introducción a la Tecnología Lonworks**, Asociación de Usuarios LonUsers España, Barcelona – España.
- ECHELON CORPORATION, **LNS DDE Server User's Guide**, Versión 2.11, Editado por Echelon Corporation, Estados Unidos de América, 1998 - 2002.
- ECHELON CORPORATION, **Guía de Diseño de Redes Lonworks**, Versión 2.1.3, Editado por Echelon Corporation, San José - USA, 2007.
- <[http://www.articulosinformativos.com/Sistemas de Control de Acceso-a862383.html](http://www.articulosinformativos.com/Sistemas%20de%20Control%20de%20Acceso-a862383.html)>, Sistemas de Control de Acceso. [En línea].
- <<http://www.virusprot.com/Art29.html>>, Detrás de la Huella. [En línea].
- <[http://www.rantring.com/seg\\_tarjM.htm](http://www.rantring.com/seg_tarjM.htm)>, Control de accesos. [En línea].
- <<http://www.taringa.net/posts/ciencia-educacion/9897059/Tecnologia->

[RFID.html](#)>, Tecnología RFID. [En línea].

- <<http://es.wikipedia.org/wiki/RFID>>, RFID. [En línea].
- <<http://domotiva.wordpress.com/2010/09/03/la-tecnologia-lonworks/>>, La tecnología LONWORKS. [En línea].
- <<http://www.forosdelweb.com/f69/fec-has-visual-basic-6-0-a-603305/>>, fechas en visual basic 6.0?. [En línea].
- <<http://www.todoexpertos.com/categorias/tecnologia-e-internet/programacion/visual-basic/respuestas/194599/hora-en-un-formulario>>, Hora en un formulario... [En línea].
- <<http://www.dreamincode.net/forums/topic/24677-connecting-to-a-sql-server-database-using-adodb/>>, Connecting to a SQL Server database using ADODB. [En línea].
- <<http://www.zonadeprogramacion.com.ar/vb61.htm>>, Visual Basic parte 6, 1) Intercambio dinámico de datos. [En línea].
- <[http://es.wikipedia.org/wiki/ActiveX\\_Data\\_Objects](http://es.wikipedia.org/wiki/ActiveX_Data_Objects)>, ActiveX Data Objects. [En línea].
- <<http://social.msdn.microsoft.com/Forums/es-AR/winforms/thread/2930d7ea-7939-4b0e-a518-4b31ced877ca>>, ADO vs ODBC. [En línea].
- <<http://www.forosdelweb.com/f69/diferencias-ado-odbc-ole-db-595201/>>, Diferencias ADO.ODBC, OLE DB. [En línea].

## 5. BIOGRAFÍA



Ricardo Javier Espín Brito, nació en la ciudad de Quito el 01 de Septiembre de 1987. Se graduó como bachiller Físico-Matemático en el “Colegio Paulo VI” en el año 2005. Terminó la Carrera de Ingeniería Electrónica, Automatización y Control en la “Escuela Politécnica del Ejército” en 2011. Desarrolló su proyecto de grado para ISDE–ECUADOR, empresa dedicada a la automatización de casas y edificios.