ESCUELA POLITECNICA DEL EJÉRCITO
DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRONICA, AUTOMATIZACIÓN Y CONTROL

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

"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"

RICARDO JAVIER ESPÍN BRITO

SANGOLQUÍ – ECUADOR

2011

CERTIFICACIÓN

Certificamos que el señor RICARDO JAVIER ESPIN BRITO, ha elaborado el proyecto de grado titulado “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” para la obtención del título de Ingeniería Electrónica, Automatización y Control, bajo nuestra dirección.

Atentamente,

_____ _____

Ing. Marcelo Escobar
DIRECTOR

Ing. Jaime Andrango
CODIRECTOR

AGRADECIMIENTO

En primer lugar quiero agradecer a Dios, por iluminarme en cada momento difícil de la vida para poder llegar hasta este punto. En segundo lugar un agradecimiento infinito a mi padres que han sido la guía necesaria para poderme forjar como un buen ser humano y un buen profesional, a este agradecimiento se suman mis hermanas que siempre han estado ahí para ayudarme con consejos y enseñanzas. También agradezco a mis abuelitos, tíos, tías, primos y primas; que nunca han dejado de ser parte fundamental en mi vida y que siempre han estado con una palabra de aliento para poder salir adelante.

Debo extender un agradecimiento especial al Director del proyecto Ing. Marcelo Escobar y Codirector del mismo Ing. Jaime Andrango que supieron guiarme de la mejor manera para el desarrollo y finalización de este proyecto.

Muchas gracias a todos.

Ricardo Javier Espín Brito

DEDICATORIA

Dedico este proyecto a mis padres por los cuales he logrado la finalización del proyecto; gracias a sus enseñanzas, consejos y reprimendas que han sabido posar en mí para tener las suficientes herramientas de enfrentar el mundo y así poder seguir creciendo. Por ustedes papi y mami es este logro, porque con este logro les digo han sido los mejores padres del mundo.

Quiero también dedicar este proyecto a mis hermanas Cristi y Pauly que han sido el complemento perfecto en mi vida y que han estado ahí en los momentos que las he necesitado. Con peleas y enojadas siempre las amaré porque son parte, no de mi vida; sino de mi corazón.

Una especial dedicatoria a mis ángeles en el cielo, la abuelita Berthita y el abuelito Jorge; responsables de las bases de mi gran familia.

Ricardo Javier Espín Brito

PRÓLOGO

En la actualidad, tanto en construcciones de casa, como edificios de oficinas o departamentos; se busca una mayor comodidad y seguridad dentro y fuera de los mismos. Hoy en día para lograr las características mencionadas en las edificaciones se tiene los llamados sistemas inteligentes los cuales integran dentro de una sola edificación varios sistemas, como son: sistemas de accesos, sistemas de alarmas (intrusión e incendios), sistemas de iluminación, CCTV (circuito cerrado de televisión) y sistemas de audio.

Existen muchos fabricantes de los sistemas mencionados pero solo algunos ofrecen en realidad una integración total de ellos, pues la mayoría solo instalan sistemas por separado sin ninguna integración parcial o total. A esta idea de integración de sistemas se le da el nombre de domótica integración de casas y de inmótica en integración de edificios.

Una de las empresas que ofrece un sistema inteligente es ISDE-ECUADOR, la cual integra principalmente sistemas de accesos, sistemas de iluminación, sistemas de alarmas de intrusión y de incendios. En el Ecuador está en pleno auge este tipo de sistemas especialmente en edificaciones nuevas destinadas para oficinas o departamentos; en donde lo primordial es la seguridad de los mismos.

En las edificaciones ya sea de oficinas o departamentos, se encuentra la necesidad de que el administrador o guardia puedan manejar el sistema desde un computador. Algo muy claro es que a los encargados de las edificaciones no se les va a enseñar cómo se programa los sistemas y cuál es su funcionamiento

interno. Pues a ellos solo les interesará el control y monitoreo de los sistemas de una forma sencilla sin muchos tecnicismos que no les competen.

Es así que se desarrolla un software con la herramienta de programación Visual Basic 6.0, para crear un programa amigable y sencillo desde el cual se pueda controlar y/o monitorear el sistema de control de accesos de una edificación que contenga máximo 50 accesos, usando el nodo de control INP-120F/V3, de la empresa ISDE-ECUADOR. Este software, permitirá tener una base de datos realizada en Microsoft Access 2007, en la cual se registrarán todos los usuarios que tendrán acceso a la edificación o recinto; como también un registro del número de puerta, la hora y fecha de los usuarios que han accedido.

Para efectos de pruebas de funcionamiento, el software se implementa en la oficina de la empresa ISDE-ECUADOR, para poder tener un control del personal y poder monitorear cuando un trabajador entra o sale de la oficina.

ÍNDICE

CAPÍTULO I

INTRODUCCIÓN

Es innegable que desde hace ya unas dos décadas el mundo vive en una revolución tecnológica, en la cual cada día se busca que las cosas se simplifiquen y al mismo tiempo den más seguridades a las personas y a sus bienes materiales. Con dicho fin se ha ido expandiendo poco a poco y con gran aceptación la llamada domótica e inmótica que no es más que la automatización de casas y edificios basados en una red de control, respectivamente; con las cuales se ofrece comodidad y seguridad en empresas y/o viviendas; con costos relativamente cómodos por las grandes ventajas que estas ofrecen a corto y mediano plazo, además de su fácil uso.

Inicialmente este tipo de automatización tuvo su cuna en Europa y en Norteamérica en donde por su conocido desarrollo y cultura, era indudable que esta tecnología iba a tener una buena aceptación. No obstante dicha tecnología desde hace ya algunos años ha llegado a Latino América en donde poco a poco se ha abierto un buen mercado principalmente siendo este a empresas que desean proteger sus bienes así como controlar el trabajo y horarios de sus empleados.

Lo cual no ocurre con la automatización de casas que ubicando en porcentajes es muy bajo en comparación con los países desarrollados, ya sea esto por la situación económica y la idiosincrasia de los latinos que no ven necesario ni útil este tipo de servicios.

Pero lo cual no indica que este servicio no tenga futuro aquí porque en todo el mundo siempre las personas buscan la comodidad y más que nada la seguridad; lo cual irá dando lugar a que más y más personas tiendan por estos servicios viendo sus ventajas.

Esto lo podemos ver concretamente en nuestro país Ecuador en el cual ya existen muchas empresas que ofrecen estos servicios que han tenido buena aceptación y que van ganando terreno principalmente en las clases media-alta y alta. Por lo cual no podemos negarnos a conocer este gran campo de la automatización que cada día nos brinda más y más beneficios. Uno de los beneficios que ofrece este servicio es el de control de accesos para una empresa o vivienda con el cual se puede controlar horarios y acceso de los empleados o personas que deseen ingresar a dichos lugares.

1.1. CONTROL DE ACCESOS

1.1.1. Introducción

El control de accesos es un sistema que cada día va ganando más mercado por la seguridad y el sin número de beneficios que este ofrece dentro de una vivienda, de una empresa o cualquier local comercial.

El control de accesos no es más que una filtración o selección de usuarios que puedan ingresar a recursos informáticos o a una infraestructura dependiendo de las necesidades. En este tipo de sistemas se maneja varios conceptos que son importantes mencionar como la **direccionalidad** entre dos puntos, es así que se puede tener estas clases de direccionalidad, como se observa en la Figura. 1.1:

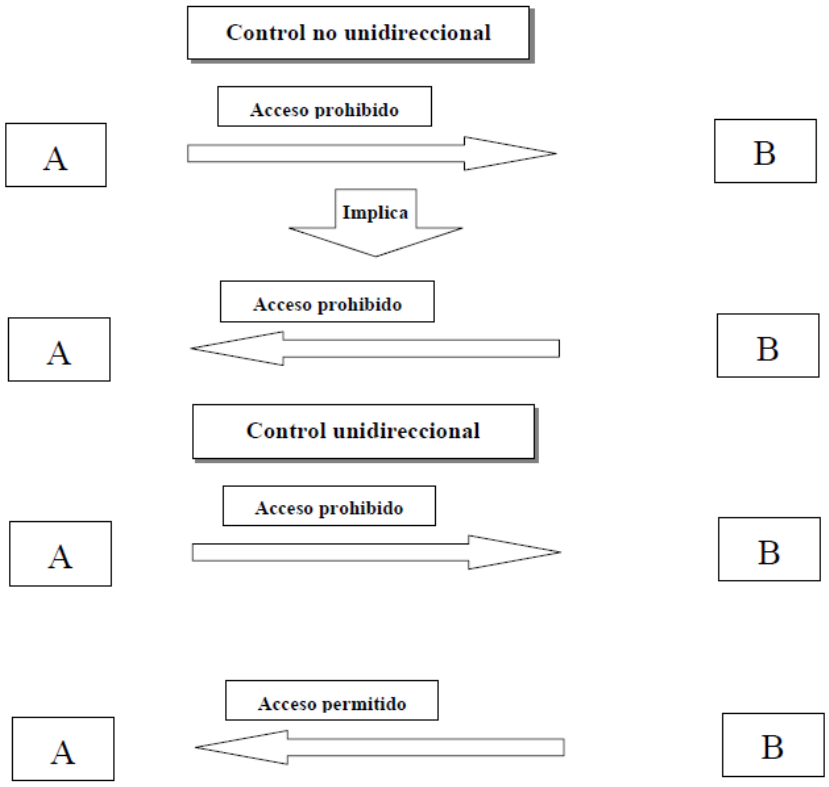


Figura. 1.1. Direccionalidad de acceso[1]

Existen dentro del control de accesos varios sistemas que pueden ser implementados para poder ofrecer este servicio; entre los cuales se pueden encontrar las tarjetas magnéticas, teclados, escáneres de huellas digitales; entre otros. Cada sistema dependerá del nivel de seguridad que se requiera y en donde se lo deba implementar.

Dentro de los beneficios que este sistema ofrece está como por ejemplo en una empresa poder controlar la puntualidad, el ingreso y salida de los empleados, así como la restricción de áreas para ciertos empleados o la restricción de personas ajenas a la empresa.

[1] PONS, Manuel, ***Control de Accesos,*** Departamento de Telecomunicaciones de la Escuela Politécnica Universitaria de Mataró, España 09 de Marzo del 2000, 42 páginas.

Este tipo de seguridad también se lo puede utilizar en edificios de departamentos, así como en locales comerciales o colegios, en donde la seguridad también es algo primordial.

Cabe señalar que este tipo de sistemas son fáciles de usar y muy rentables ya que ya no sería necesario la contratación de guardias y/o personal que controle la entrada o salida de empleados o personas a un sitio determinado.

1.1.2. Control de acceso autónomo

Figura. 1.2. Módulo de control de accesos

Los sistemas de control de acceso autónomo o también conocidos como “Stand Alone”, son aquellos que no necesitan de un software para poder controlar el funcionamiento del equipo. “Es el propio equipo quien gestiona el acceso de manera autónoma”.[2]

Este es un solo equipo compacto, fiable y utilizado en muchos lugares que funciona independientemente, es decir aquí mismo se configura las restricciones de acceso y la identificación de los usuarios que tienen accesos, además se tiene una base de todos los ingresos y salidas de los usuarios permitidos dentro de sí mismos. Y existe la posibilidad de ingresar al equipo, obtener estas bases y configurarlo con un software especial para determinado equipo; pero siendo esto con una comunicación única entre el equipo y el software en un computador.

[2] http://www.kimaldi.com/area_de_conocimiento/control_de_acceso_y_presencia/funcionamiento_autonomo_stand_alone_offline_online, Control de acceso y presencia.

1.1.3. Control de acceso no autónomo

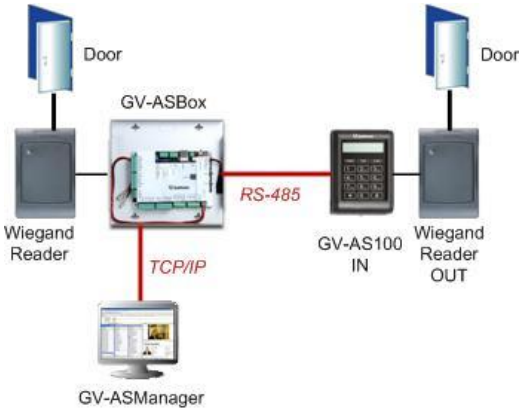


Figura. 1.3. Red de control

Los sistemas de control no autónomo son aquellos que para su control necesitan conectarse a un servidor, desde donde el cual se realiza todo el control y la configuración de cada uno de los accesos.

Aquí todos los controladores de cada uno de los accesos se encuentran conectados en red dirigidos a un solo servidor desde el cual todos son controlados.

El enlace entre los controladores se lo realiza mediante el protocolo que soporten los controladores de acceso que se estén utilizando, y para la conexión de los controladores mencionados a los respectivos sensores como: de proximidad o huella digital; se lo hace mediante el protocolo Wiegand.

1.1.4. Protocolo Wiegand

El inicio del protocolo Wiegand nace a partir del conocido efecto Wiegand, que “es un concepto físico en el que intervienen las distintas formas de reaccionar

magnéticamente distintas áreas de un hilo conductor ante la influencia de un campo magnético."[3]

En base a este efecto se crean tarjetas de identificación con sus lectores de proximidad para este tipo de tarjetas en sistemas de control de accesos o de presencia. Como es de suponer los lectores se deben conectar de alguna forma a los sistemas de control de accesos para poder comunicarlos; por ello es que se crea el protocolo de comunicación Wiegand.

"El término del interface **Wiegand** es una marca de la sociedad "Sensor Engineering Company" y fue diseñado para conseguir una tecnología que permitiera transmitir datos de un identificador (tarjeta) entre dos dispositivos alejados entre sí, como, por ejemplo, un lector y la central de control de accesos. El protocolo Wiegand es ampliamente utilizado por la mayor parte de los fabricantes porque permite la transmisión de información a través de un par de cobre que se acompaña de la alimentación para el dispositivo de lectura sin afectar por ello a los datos."[4]

Los 0 y los 1 son unos impulsos de entre 20 µs à 100 µs de duración en su estado bajo. El interface se completa con 5 bornes, con la codificación siguiente:

- ✓ Rojo: alimentación (5 V ó 12 V ó 24 V nominal).
- ✓ Negro: comun (masa)
- ✓ Blanco: data 1
- ✓ Verde: data 0
- ✓ Marrón: control de LED

[3] http://picmania.garcia-cuervo.net/conceptos_wiegand.php, El Protocolo Wiegand

[4] http://control-accesos.es/protocolos/protocolo-wiegand, Protocolo Wiegand

La normativa autoriza hasta 153 m. de cable de cobre de diámetro 1,02mm (0,82 mm2 correspondiente a un cable AWG 18). El protocolo de comunicaciones Wiegand consta de dos partes fundamentales que son:

- Modo físico de transmisión de la información
- Interpretación numérica de la información

Modo físico de transmisión de la información

Sistema de transmisión

Es una transmisión de modo asincrónico, la cual se realiza por intermedio de tres hilos. Los niveles con los que trabajan son nivel el bajo que está a nivel de tierra (GND), y nivel alto a +5(V). El envío de datos por los tres hilos es el siguiente:

- **DATA 0:** Línea que envía los ceros lógicos.
- **DATA 1:** Línea que envía los unos lógicos.
- **GND:** Línea a masa de referencia de DATA 0 y DATA 1.

Existen tres estados que ocurren que son:

- El estado de reposo donde no se trasmite, la línea GND está en bajo y las líneas DATA 0 y DATA 1 están en alto.
- Para trasmitir un bit 1 se debe enviar un pulso a nivel bajo con una duración de 50 us por la línea de DATA 1, mientras la línea DATA 0 se mantiene en alto.
- Para transmitir un bit 0 se produce el proceso contrario ya que ahora se envía un pulso a bajo por la línea de DATA 0 con duración de 50 us, mientras la línea de DATA 1 se mantiene en alto.

El tiempo de duración entre cada pulso y el siguiente es de 2ms.

Representación de la transmisión de la secuencia de bits ***1010,*** Figura. 1.4.

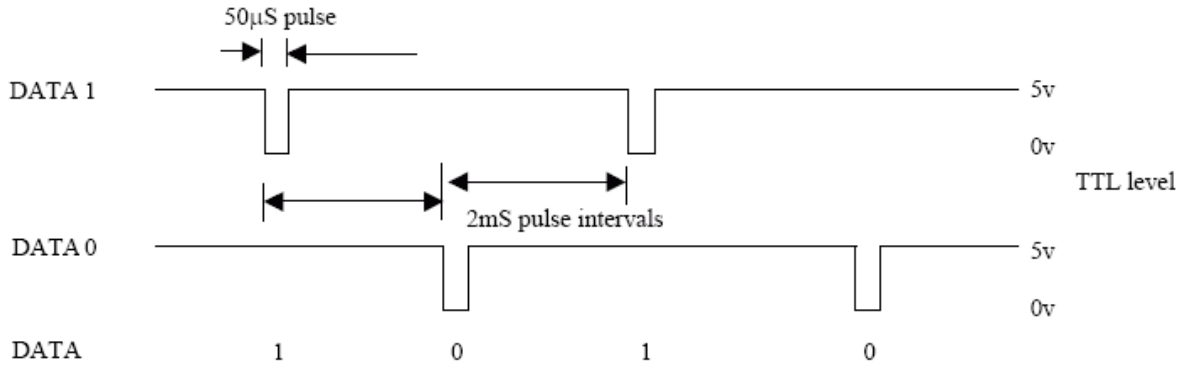


Figura. 1.4. Diagrama de transmisión

Interpretación numérica de la información

Mediante el modo de transmisión físico que se indicó con anterioridad se pueden trasmitir tantos bits como se requieran pero se han llegado a estándares como son de: 26, 32, 44 ó 128 bits. Siendo el primero el Wiegand de 26 bits el más utilizado y el que se lo interpreta de una sola forma, ya que existen los otros modos que se los interpreta de muchas formas por lo distintos fabricantes que manejan este protocolo.

- A continuación, se explica la interpretación del método de transmisión Wiegand de 26 bits.

- El primer bit, B0 es el bit de paridad par de los primeros bits transmitidos del B1 – B12.
- Facility code, bits del B1 – B8 que es igual a un byte.
- User code, bits del B9 – B24, que es igual a dos bytes.
- El último bit, B25 es el bit de la paridad impar de los últimos bits transmitidos del B13 – B24.

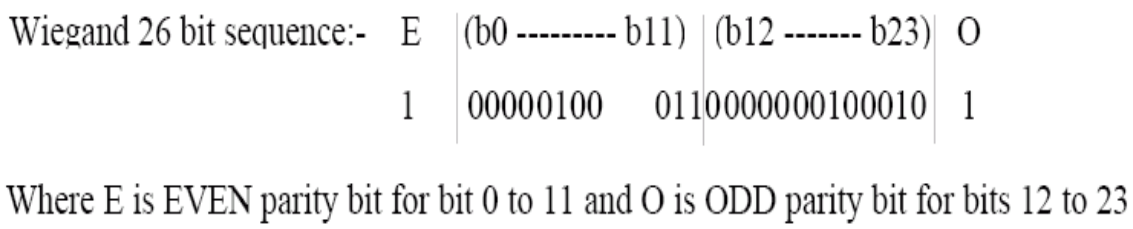


Figura. 1.5. Representación Wiegand 26 bits

Como se observa en la Figura. 1.5., E es 1 para dar la paridad par a los primeros 12 bits ya que tienen tres unos; y así se tiene que O también es 1 para dar la paridad impar a los últimos 12 bits que tienen dos ceros.

- Interpretación del Wiegand 32 bits

Este modo no lleva bits de paridad, en donde el Facility y User Code son de 16 bits cada uno; es decir, 2 bytes cada uno.

- Interpretación del Wiegand 44 bits

Modo que tampoco lleva bits de paridad, en donde el Facility Code tiene 8 bits y el User code tiene 32 bits, siendo los últimos 4 bits la OR EXCLUSIVA de los 40 bits anteriores tomados de 4 en 4. Permite numeración desde 1 a 65.535. Para permitir un mayor número de tarjetas, sin duplicaciones, se agrega un extra código de tres dígitos, llamado "Sitio" o "Edificio".

Beneficios

No es necesario ordenar tarjetas con estos códigos especiales. Desde que estos códigos son específicamente asignados, es difícil conseguir remplazos y agregados; por lo tanto, hay demoras e inconvenientes cuando se precisan nuevas tarjetas.

La mayoría de los fabricantes (OEM) tienen una estructura de bits propia en protocolo Wiegand. Con la versión genérica de 26 bits existe un pequeño riesgo de duplicación a diferencia de un protocolo de 36 bits; por lo tanto, el nivel de seguridad es un poco más bajo que los formatos únicos.

1.1.5. Tipos de sistemas de control de accesos

- **Métodos biométricos**

Figura. 1.6. Módulo biométrico

Este tipo de sistemas se dan gracias a los métodos biométricos de identificación los cuales ayudan a detectar características propias de cada una de las personas como son la huella digital, el iris del ojo o el tono de voz. Como por ejemplo para las huellas digitales se toman puntos característicos de las huellas para posteriormente ser comparada, de esta manera la información dactilar ha sido reducida solo a un algoritmo matemático.

Siendo el primero de estos el más utilizado en las empresas ya que con estos sistemas con solo pasar uno de sus dedos registrados en el sistema de identificación se puede identificar si un determinado empleado ha llegado al trabajo o de la misma manera cuando este haya salido.

- **Magnetismo**

Figura. 1.7. Módulo para tarjetas magnéticas

Este tipo de sistemas constan de tarjetas magnéticas que son identificadas por un lector de dichas tarjetas. Cada una de las tarjetas contiene un código único, el cual se lo usa para ingresarlo al sistema y solo el que posea dicha tarjeta tendrá acceso a una puerta o varias puertas al que se deba permitir el acceso.

Mediante un software se puede ingresar el código antes mencionado, además de realizar algunas configuraciones más como por ejemplo determinar un determinado horario de activación de las tarjetas generalmente utilizado en las empresas en donde los empleados solo tendrán un intervalo de tiempo para poder ingresar. Además en dicho software se puede llevar un registro de cuántas veces ha pasado una determinada tarjeta.

- **T**eclados

Figura. 1.8. Teclado

En estos sistemas a cada uno de los usuarios se le asigna un usuario y una contraseña con los cuales pueden registrar su llegada y así ver si están registrados y el sistema permite o no el ingreso de la persona.

Como en los otros sistemas también se va registrando las horas y la persona que ha ingresado.

- RFID (125KHz y 13,53MHz)

Figura. 1.9. Lector de proximidad

Las siglas en inglés RFID significan Radio Frequency Identification. Este es un sistema de almacenamiento y recuperación de datos remotos que usa dispositivos denominados tarjetas, transpondedores, etiquetas o tags RFID. El propósito principal de esta tecnología es transmitir la identidad única de un objeto mediante ondas de radio. Las tecnologías RFID se agrupan dentro de las denominadas Auto ID (identificación automática).

Estos dispositivos contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID el cual se lo conoce como lector de proximidad, especialmente cuando se refiere a un sistema de control de accesos. El tipo de antena utilizado en un tag depende de su aplicación y de la frecuencia de operación. Los tags de baja frecuencia (150Khz) normalmente se sirven de la inducción electromagnética. Como el voltaje inducido es proporcional a la frecuencia, se puede producir el necesario para alimentar un circuito integrado utilizando un número suficiente de espiras. Existen tags de baja

frecuencia compactos (como los encapsulados en vidrio utilizados para identificación humana y animal) que utilizan una antena en varios niveles (tres de 100-150 espiras cada uno) alrededor de un núcleo de ferrita.

En alta frecuencia (13,56 MHz) se utiliza una espiral plana con 5-7 vueltas y un factor de forma parecido al de una tarjeta de crédito para lograr distancias de decenas de centímetros. Estas antenas son más baratas que las de baja frecuencia ya que pueden producirse por medio de litografía en lugar de espiración, aunque son necesarias dos superficies de metal y una aislante para realizar la conexión cruzada del nivel exterior al interior de la espiral, donde se encuentran el condensador de resonancia y el circuito integrado.

1.1.6. Sistema anti-passback

- **Introducción**

Anti-passback es el nombre que se lo da a un sistema que impide que la acreditación de una identificación pueda usarse en más de una ocasión para poder acceder a algún lugar sin que se haya producido la salida; y viceversa, el objetivo es que el propietario de una tarjeta no pueda ceder esta a una segunda persona para que tenga también acceso.

Este tipo de control además de ser aplicados con las tarjetas de proximidad también se los aplica en la huella digital.

Un ejemplo claro que se puede mencionar es en el parqueadero de oficinas o departamentos, en donde debe existir un rígido control del acceso al mismo como el control de los espacios para el parqueamiento; con este sistema anti-passback se ayuda a que solo ingrese el dueño de la tarjeta y nadie más.

"Con cualquier sistema de **Anti-PassBack** se utiliza el concepto de **"disponibilidad de un lector"**. Esto significa simplemente la posibilidad de identificar si un lector en particular está como '**entry**' (entrada), '**exit**' (salida), '**internal**' (interno), o '**don't care**' (no importa). Cuando los lectores son asignados como entradas o salidas los sistemas tienen la posibilidad de registrar, si un usuario está dentro o fuera en cualquier momento simplemente conociendo donde fue la última vez que se identificó.

Si la última vez que **se identificó fue en un lector de salida** entonces el sistema sabe que **está fuera**.

Si la última vez que **se identificó fue en un lector de entrada** entonces el sistema sabe que **está dentro**."[5]

Anti-passback local: Cuando el sistema realiza anti-passback sobre los accesos controlados por una única central.

Anti-passback global: Cuando el reconocimiento es a nivel de todas las centrales o controladores.

- **Tipos de anti-passback**

Anti-passback duro

El sistema utiliza la situación individual de cada usuario para determinar si es permitido el uso de un lector en particular. Los lectores son designados como entrada, salida ó no me importa; así el sistema sabe si los usuarios están adentro o afuera. Anti-passback duro les impide utilizar su tarjeta para entrar en los locales si ya están dentro, o salir si ya están fuera.

[5] http://www.aplicacionestecnologicas.com/Control_de_Acceso/Anti_PassBack/index.html, Anti-passback

Con este tipo de anti-passback, los usuarios no pueden "pasar de nuevo" su credencial para que otra persona entre con la misma credencial porque una vez que ha entrado en el sistema sabe quién está dentro y no le permitirá un nuevo acceso a menos que el usuario vuelva a salir.

El anti-passback duro mantiene un alto nivel de seguridad, pero puede causar molestias en los usuarios que se olviden de utilizar su tarjeta para entrar o salir ya que si cometen el error de entrar con otro usuario sin usar su tarjeta ya no podrán volver a salir porque el sistema les detectará como que nunca han entrado o de la misma manera si salen no podrán entrar.

Anti-passback suave

Con anti-passback suave el sistema registra el estado de cada usuario, por lo tanto sabe si el usuario está dentro o fuera de algún lugar, pero no tiene ninguna restricción de acceso. Así, si se encuentra dentro y tratar de volver a entrar el sistema le permitirá el acceso.

Puede ser menos preciso, ya que no se ha impuesto que los usuarios deben introducir la tarjeta antes de salir, y viceversa. Es por lo que también reduce la seguridad, el sistema sabe donde está una persona, pero no que dejen entrar dos veces. Este tipo de sistema se utiliza a menudo con la asistencia y aplicaciones de tiempo.

Perdonar a un usuario

Los usuarios pueden tener tres posibles estados en un sistema de anti-passback que son: interior, exterior o desconocido.

"Perdonar" a un usuario simplemente significa establecer su estado antipassback de nuevo a "desconocidos" para que la próxima vez que intente

entrar o salir este podrá realizar su acción sin ningún problema pues el sistema no sabe donde se encuentra el usuario.

Tailgating

Término que se refiere a un usuario que ingresa después de otro usuario a través de una puerta o boomgate sin presentar una credencial. Ambos cruzan la puerta juntos pero sólo el primer usuario se registra como estar dentro o fuera.

Violación de passback

Término que se refiere cuando un usuario tiene su estado de anti-passback incorrecto; es decir, que su estado indica estar afuera o adentro pero el está realmente en el estado contrario.

Anti-passback programado

Este tipo de sistemas es cuando un usuario es perdonado, dicho de una manera más clara el estado del usuario cuando ha entrado a algún lugar; después de un tiempo determinado, cambia a su estado original o simplemente se lo pone en estado desconocido, para que luego la tarjeta pueda ser utilizada para que alguien más ingrese.

Es muy bueno en cuestión de ahorro pues así no se necesita un lector de salida.

Anti-passback mundial

Este tipo de anti-passback se lo realiza cuando el registro de un usuario dentro de un controlador de una red envía la información a otros controladores de la misma red, así de esta forma el usuario podrá estar registrado en cada uno de los accesos.

Es decir si un usuario es detectado que en un acceso está dentro no podrá ingresar en algún otro acceso, pues estará registrado como que no ha salido de de otro lugar.

Recibir reporte

Es algo muy importante dentro de la seguridad de un edificio o establecimiento, especialmente cuando se ha producido algún incidente dentro de este cómo pueden ser incendios o derrumbes. Con este sistema se puede obtener un listado de la gente que se encuentra dentro de la estructura y así determinar acciones correspondientes.

1.1.7. Software

Figura. 1.10. Software de control

Los sistemas de control de accesos para poder llevar a cabo la configuración y supervisión del Hadware que proveerá de los mencionados sistemas, necesitan de un software con el cual se realice dicho proceso. Según las funcionalidades que necesite su sistema de control de accesos deberá escoger entre soluciones Off-line u, On-line.

Algunas de las más importantes configuraciones que suelen realizarse:

- Definición de grupos de acceso y zonas horarias
- Completa información de los usuarios
- Control de visitantes
- Visualización de eventos y transacciones
- Múltiples eventos de alarmas
- Monitoreo gráfico de alarmas
- Contadores de eventos
- Control con máxima seguridad
- Interfaz de servidor OPC
- Base de datos de todas las operaciones antes mencionadas

Algún software de estos sistemas es modular y escalable a los tamaños de las empresas y según las funciones que estas necesitan.

Características generales de softwares de control de accesos

- Sistemas de control de accesos "mono-aplicación".
- Sistema de seguridad integrado con aplicaciones de seguridad contra intrusiones y video-vigilancia para la supervisión y el control de lugares y personas en tiempo real.
- Gran sistema de seguridad y control de tiempo que gestione cientos de terminales y puertas en una arquitectura perfectamente compatible con la política corporativa en términos de seguridad de redes e integridad de la información.

Se podría hablar de algunos tipos de software para los sistemas de control de accesos, ya que se pueden tener softwares especiales para la infraestructura donde estos sistemas serán instalados. Entre los cuales se pueden mencionar: Empresas, viviendas, centros deportivos, centros comerciales, etc. Cada uno

tendrá sus características específicas para la solución que se requiera dar en determinado sitio.

1.1.8. Sistemas complementarios

Los sistemas de control de accesos como se lo ha mencionado son muy útiles cuando en cuestión de seguridad se refiere, por lo mismo estos sistemas dan posibilidad de integrarse con otros sistemas que son un complemento para aumentar la seguridad y así obtener un sistema completo de seguridad.

Por ejemplo se pueden integrar con sistemas de seguridad de alarmas o de iluminación, así como un circuito cerrado de televisión que incrementa el control dentro de una empresa o edificación en la cual se instale.

1.1.9. Costos

Al hablar del precio de este tipo de sistemas inmediatamente se piensa en valores exagerados y que no vale la pena invertir en ellos lo cual no tiene nada de cierto ya que el costo de estos sistemas son relativamente bajos en comparación con los altos beneficios que estos ofrecen ya sea en cuestión de seguridad y de comodidad.

Además es importante mencionar que el costo depende del nivel de seguridad que se desee. Estos pueden variar si se quiere un teclado, un sistema de lector magnético o un sistema de identificación biométrica.

Además se debe tomar en cuenta también el tamaño de lugar donde se implementa a este sistema de control de accesos, pues puede variar en el número de puertas que serán aseguradas.

Por todo lo mencionado, un sistema de control de accesos es un sistema destinado a la seguridad de cualquier edificación cuya implementación, costo y operatividad dependerá del lugar y del nivel de seguridad que se desee implementar. Tomando en cuenta todos los beneficios que esto conlleva y las diferentes ofertas que existen en el mercado para dichos sistemas.

1.2. INTRODUCCIÓN DE TECNOLOGÍA LONWORKS

1.2.1. Introducción

Dentro de todos los sistemas de automatización que se ofrecen existen muchos protocolos los cuales son muy usados por los integradores.

Entre los cuales se pueden encontrar protocolos:

- Propietarios
- Estándares

a. Propietarios o cerrados

Con estos protocolos solo se pueden trabajar con los fabricantes de una sola marca, no se pueden integrar con otros fabricantes.

Todos los sistemas centralizados y algunos sistemas distribuidos trabajan con protocolos cerrados o propietarios. A este tipo de protocolos se les puede señalar ventajas y desventajas como las siguientes:

Ventajas:

- Generalmente equipos más baratos.

Desventajas:

- Gran dependencia a un solo fabricante.
- Altos costos de mantenimiento.
- Indisponibilidad de repuesto en caso de cierre de la empresa que fabrica los dispositivos.

Algunos de los protocolos propietarios que existen:

- SIMON
- AMIGO
- VIVIMAT
- COMUNITEC
- BTICINO
- VANTAGE
- LUTRON
- THUNDER

b. Estándares o abiertos

Este tipo de protocolos son creados para poder ser integrados con diferentes fabricantes, los cuales presentan más ventajas que los protocolos propietarios.

Este tipo de protocolos son reconocidos por algún organismo de normalización, y presentan las siguientes ventajas:

Ventajas:

- Bajos costos de mantenimiento.
- Diversidad de productos.
- No depender de un solo fabricante.
- Flexibilidad, escalabilidad.

- Tecnologías certificadas por diversos institutos de estandarización, lo que garantiza la calidad de los sistemas.

Aquí algunos de los protocolos de estándares o abiertos:

- Lonworks
- X10
- KNX – EIB
- BAC – net
- Zigbee
- Batibus

1.2.2. ¿Qué es una red de control?

Una red de control es la que está formada por dispositivos de control como los sensores o actuadores integrados para una determinada aplicación. En una red de control todos estos dispositivos se integran o comunican mediante normas o protocolos de comunicación.

Cada uno de estos dispositivos de la red de control se lo llama nodo; estas redes se las utiliza generalmente para aplicaciones de monitorización y control.

Cada uno de los dispositivos de la red están en la capacidad de enviar y recibir pequeños mensajes para el control de los mismos, a estos mensajes de control se los llama variables de red o se les puede llamar “NVs” que es la abreviación de su significado en inglés “Network variables”.

Existen dos tipos de redes a considerar en estos sistemas que son:

- Sistema de control maestro/esclavo
- Sistema de control punto a punto

a. Sistema de control maestro/esclavo

En este tipo de sistemas existe un controlador que actúa como el maestro al cual se conectan todos los dispositivos, sensores, actuadores que se quieren controlar; siendo estos los esclavos.

Este tipo de sistemas tiene características importantes que se deben valorar al momento de decidirse por un sistema de este tipo.

Características:

- Hay un único punto de falla general en el sistema
- Muy difícil su escalamiento
- Costo elevado en cableado
- Programación propietaria
- Soluciones propietarias

b. Sistema de control punto a punto

Este es un tipo de sistema distribuido donde cada uno de los dispositivos actuadores, sensores; tienen su propio controlador; los cuales no necesitan de un controlador principal como en el sistema maestro/esclavo.

Este tipo de sistemas tiene características importantes que se deben valorar al momento de decidirse por un sistema de este tipo.

Características:

- El control se realiza donde está el elemento a controlar
- No existe ningún tipo de fallo general en el sistema cada uno es independiente.
- Es escalable

- Es menos costoso en cableado
- Permite integración con distintos fabricantes

1.2.3. Plataforma Lonworks®

"Lonworks® es una plataforma de control creada por la compañía norteamericana Echelon. Las redes Lonworks® describen de una manera efectiva una solución completa a los problemas de sistemas de control."[6]

Este tipo de tecnología es un **sistema estándar con norma ISO** que ofrece muchas soluciones para distintos tipos de diseños y arquitecturas y mantenimiento de redes de control, dichas redes pueden ser muy grandes pudiendo tener de 2 a 32000 dispositivos. Pudiendo ser utilizada desde una vivienda particular hasta una gran industria; incluso hasta en vehículos, aviones y barcos.

Lonworks es una tecnología que permite una gran interoperabilidad, compatibilidad y escalabilidad es sus sistemas. Tratando así de que se vaya quitando la tendencia de obtener sistemas propietarios, con una tecnología robusta además de económica y fácil de usar.

"El comienzo de las redes Lonworks® se basó en conceptos muy simples:

1) Los sistemas de control son fundamentalmente idénticos, independientemente de la aplicación final.
2) Un sistema de control distribuido es significativamente más potente, flexible, y ampliable que un sistema de control centralizado.
3) La empresas ahorran más dinero a largo plazo instalando redes distribuidas que instalando redes centralizadas."[7]

[6] LonUsers – España, ***Introducción a la Tecnología Lonworks***, Asociación LonUsers – España, 11 páginas.

[7] LonUsers – España, ***Introducción a la Tecnología Lonworks***, Asociación LonUsers – España, 11 páginas.

Este tipo de tecnología la podemos encontrar en aplicaciones específicas como son: control de producción, seguimiento de artículos, entornos de trabajos automatizados, control medio ambiental, gestión de energía, control de peajes, sistemas de identificación y las aplicaciones de seguridad en las viviendas particulares y empresas.

1.2.4. Origen de plataforma Lonworks

La tecnología Lonworks está basada en el pensamiento de AC “Mike” Makkula quién es cofundador y ex-director de Apple Computer.

La idea era que los ordenadores puedan ser embebidos en todos los dispositivos, para que de esta forma la inteligencia de un sistema pueda ser distribuida.

Es así que Echelon, fundada en 1988, crea el primer Neuron Chip en 1991; quién desarrolló y publicó el protocolo europeo Lontalk que después pasaría a ser el protocolo europeo ANSI/EIA 709.1 – C, con norma ISO - 14908. Protocolo de comunicaciones estándar y abierto.

1.2.5. Ventajas de la plataforma Lonworks

- Se trata de un protocolo de redes de dispositivos robusto, fiable y probado disponible en un chip.
- Los fabricantes de dispositivos inteligentes pueden llegar al mercado rápidamente.
- Los usuarios finales ya no están obligados a tener un único proveedor de tecnología.
- Los integradores pueden elegir los dispositivos más apropiados dentro de una gran gama.
- El protocolo Lontalk ANSI/EIA 709.1-EN 14908 es independiente del medio de transmisión.

- Las herramientas Lonworks operan sobre múltiples plataforma.
- Existe un grupo de estándares multi-industrial, Lonmark Internacional, para asegurar interoperabilidad.

1.3. TECNOLOGÍA LONWORKS

1.3.1. Control de Lonworks

El control Lonwork es un control distribuido, donde cada nodo de una red de control Lonworks tiene un microprocesador que se comunica por medio del protocolo europeo ANSI/EIA 709.1, con norma ISO - 14908; cada nodo subdivide sus actividades de control en funciones las cuales toman el nombre de bloques funcionales, estos bloques pueden ser considerados como una entrada, una salida, un controlador o una función genérica del sistema.

Cada nodo envía y recibe pequeños paquetes de mensajes que contienen datos de control. Los datos de control reciben el nombre de variables de red o “Network variables” o NVs. Los bloques funcionales definen las variables de red que son necesarias para cumplir con su función.

1.3.2. Programa de redes Lonworks

Programar una red es cuando se especifica que bloque funcional de la red intercambia datos a través de las variables de red; estos bloques funcionales pueden estar implementados en redes grandes, potentes y flexibles siendo estas redes de área local (LAN) y/o redes de área extensa (WAN).

El control de Lonworks es un proceso dirigido por eventos. Existe una imagen de red que consta de un conjunto de dispositivos configurados y sus uniones de variables de red. Es necesario de una herramienta de red para configurar el comportamiento de un dispositivo y definir las conexiones de variables de red.

Una vez que se completa la configuración dicha herramienta de red se la puede retirar y la red puede seguir funcionando por sí sola.

La herramienta de red asigna un número o identificación lógica única a cada dispositivo para que los paquetes de mensajes sean aislados y redirigidos por routers inteligentes Lonworks.

Se puede integrar información de dispositivos a través de una red de cualquier tamaño, incluso a través del internet; ya que el protocolo de Lontalk ANSI/EIA 709.1 es escalable.

1.3.3. Protocolo de Lonworks

El protocolo que usa la tecnología Lonworks es un protocolo abierto que permite integración con dispositivos de distintos fabricantes.

El protocolo es el Lontalk ANSI/EIA 709.1 – EN 14908, diseñado para aplicaciones de control y no para aplicaciones de datos.

El protocolo se basa en las 7 capas del modelo estándar OSI para comunicaciones de red, el protocolo es implementado en un Neuron Chip; así como puede ser implementado en cualquier procesador equivalente, por su mencionada interoperabilidad.

El protocolo es independiente del medio de transmisión y es un estándar abierto, publicado y disponible para cualquiera.

1.3.4. Elementos de un red Lonworks

- **Objetos físicos de una red Lonworks**

Constan de:

- Dispositivos inteligentes o nodos, certificados por Lonmark:

  - Actuadores
  - Sensores
  - Controladores
  - Combinación de actuadores, sensores y controladores
  - Ruoters

- Medio de transmisión de la red para transporte de comunicaciones:

  - La mayoría de los dispositivos usan par trenzado sencillo, como el de categoría 4, o líneas de potencia.

- Herramientas de red:

  - Crear el programa de red, comisionar dispositivos, probar, verificar y mantener la red.
  - Las herramientas HMI son usadas para monitorizar y controlar condiciones de la red, notificar alarmas, obtener datos y dotar de programación horaria a los equipos.
  - Las herramientas de análisis de protocolo verifican el ancho de banda de la red, proporcionan análisis estadístico y sirven como herramientas de resolución de problemas.

- **Objetos lógicos en una red Lonworks**

Bloques funcionales

Un bloque funcional es aquel que tiene la función que realizará el dispositivo, el cual podrá contener varios bloques funcionales ya que puede realizar varios eventos. Cada bloque funcional está compuesto por variables de red y propiedades de configuración.

La asociación Lonmark define plantillas “Templates” estándares para los bloques funcionales llamados perfiles funcionales estándares o SFPs.

Variables de red

Son los datos enviados y recibidos por los dispositivos de una red, dicha información puede ser de señales como temperatura, presión, volumen, etc.

Lonmark define *tipos de variables de red estándares* para fomentar la interoperabilidad, dándoles a así a cada variable de red estructura, tamaño, rango; conocidos y documentados.

Puede suceder que estos tipos de variables de red creados por Lonmark no cumplan con ciertas necesidades de dispositivos que son hechos por diferentes fabricantes, por lo que cada uno de ellos crea su propio *tipo de variable de red de usuario;* los cuales deben estar definidos de una manera estándar, y los ficheros de formatos proporcionados por el fabricante deben definir el formato del dato para una herramienta de red, entonces así puede cumplir con los requerimientos de Lonmark.

Propiedades de configuración

Estos son valores configurables por el usuario que definen el comportamiento del dispositivo tales como: punto de consigna, límite máximo o throttle.

Al igual que las variables de red Lonmark crea *tipos de propiedades de configuración estándares* que fomentan la interoperabilidad y que tienen una estructura, formato, rango; conocidos y documentados.

Y así mismo los dispositivos de distintos fabricantes que no se satisfacen con los tipos definidos por Lonmark, crean sus propios *tipos de propiedades de configuración de usuario*. El fabricante en cuestión debe aportar ficheros de formato para presentar los valores a la herramienta de red.

1.3.5. Servicios de red Lonworks

También conocidos como *LNS,* es una plataforma para redes multi vendedores interoperables.

- **Ventajas:**

  - Dota de un kit esencial de herramienta de gestión y opciones de conectividad.
  - Es una arquitectura cliente/servidor.
  - Permite coexistir en una misma red a múltiples herramientas de red de múltiples puestos.
  - Provee la habilidad de conectar redes sobre IP.
  - Dota de una arquitectura para construir herramientas de red personalizadas, incluyendo Plug-ins de red y de dispositivos.

1.3.6. Arquitecturas de redes

Existen muchas arquitecturas de red que se verán a continuación, teniendo cada una de ellas ciertas características que satisfacen las necesidades de una determinada red que se requiera. Entres estas características podemos encontrar:

- El tamaño de la red
- El tipo de estructura en que se implementará ya sea casa, edificio, etc.
- Si la red ejecuta un proceso de manufacturación a través de múltiples partes de los equipos.
- Si la red está auto contenida en una parte de los equipos.

- **Arquitectura básica**

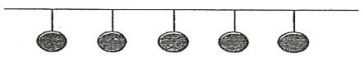


Figura. 1.11. Arquitectura básica

Consta de un sistema de control abierto y distribuido que incluye sólo dispositivos Lonworks sin puesto de control alguno ni herramienta de gestión de redes permanentes

Ventajas:

- Bajos costos.
- No se requiere un puesto de control permanente.

Deventajas:

- Requiere disponer de una herramienta de gestión de red y de la versión actualizada de la base de datos de la red in-situ cuando se añadan, muevan o cambien de la red.
- No está disponible una interfaz de usuario.

- **Sistema básico con gestor de dispositivos embebidos**

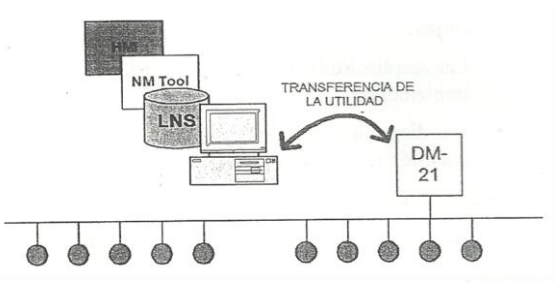


Figura. 1.12. Gestor de dispositivos embebidos

A diferencia de la anterior arquitectura, está consta de gestión local y tareas de supervisión del sistema por medio de un PC externo a la instalación. Se usa una herramienta de transferencia para pasar la base de datos al gestor de dispositivos.

Ventajas:

- Bajos costos, tiene control y supervisión de dispositivos in-situ.
- Soporte de sustitución automático.
- Sistema escalable.

Desventajas:

- Sincronización de la base de datos manual (Herramienta de transferencia).
- Los cambios a través del gestor de dispositivos no son inmediatos.
- No hay disponible un puesto de control.

- **Sistema básico con herramientas de gestión de red ubicadas localmente**

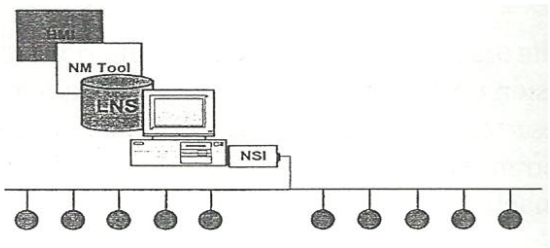


Figura. 1.13. Gestión de red ubicadas localmente

La estación de trabajo operadora incluye el sistema operativo de la red, una herramienta de gestión de red y un HMI (interfaz hombre-máquina) ejecutándose en un PC local.

Ventajas:

- Las ampliaciones, movimientos y cambios en la instalación son rápidos de implementar.
- Los diagramas de la red y las bases de datos se mantienen de la misma manera que fueron construidos.

Desventajas:

- Requiere un PC permanentemente en la instalación.

- **Arquitectura cliente/servidor sencilla**

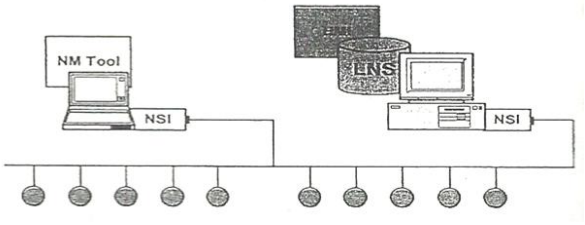


Figura. 1.14. Arquitectura cliente/servidor sencilla

Consta de una estación de control local en el que corre el servidor de la red, además de aplicaciones HMI. El cliente local corre en un ordenador portátil quién ejecuta una herramienta de gestión de red.

En el servidor va la aplicación LNS para permitir la comunicación entre la herramienta de cliente y LNS.

Ventajas:

- Permite a multitud de herramientas remotas acceder simultáneamente a los datos de la red y gestionar dispositivos a través de los medios de comunicación existentes en la red.

Desventajas:

- A medida que aumenta el tráfico de red entre las herramientas cliente y servidor se degrada el funcionamiento de la red.

- **Arquitectura de cliente “Lightweight”**

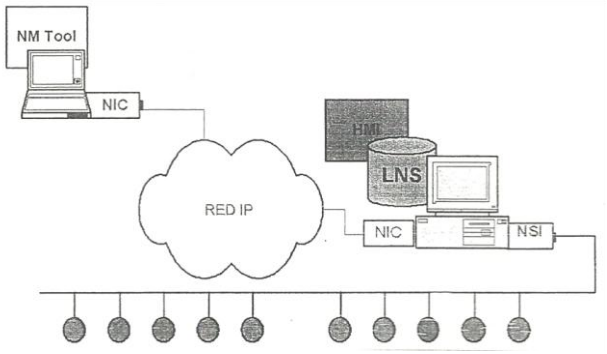


Figura. 1.15. Lightweight

El cliente se conecta con el servidor LNS vía Ethernet para llevar a cabo la gestión, monitorización y tareas de control de la red.

Ventajas:

- Todo el tráfico cliente – servidor se da sobre IP, dando así una comunicación más rápida y sin impacto negativo en el tráfico de la red.

Desventajas:

- Se puede formar una congestión de datos en el servidor LNS ya que todos los datos del cliente son enrutados a través del servidor.

- **Arquitectura cliente "Full"**

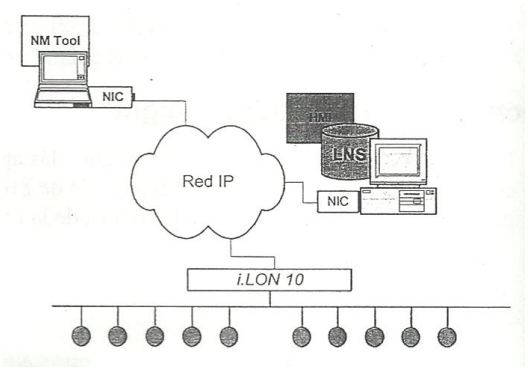


Figura. 1.16. Full

Como en la arquitectura anterior el cliente se comunica al servidor LNS vía Ethernet pero solo para tareas de gestión de red; para monitorización y tareas de control el cliente se comunica directamente con los dispositivos de red a través de un interfaz de red remoto.

Ventajas:

- La base de datos de la red es mantenida desde el exterior de la red en un centro de datos seguro; no se necesita PC en la red.
- Si el servidor no está disponible las aplicaciones del cliente pueden acceder directamente a la información de los dispositivos creando aplicaciones redundantes de monitorización y control.
- Existen interfaces de red remotos y baratos como el adaptador a Ethernet i.LON 10.
- Las alarmas pueden ser reportadas a varias aplicaciones LNS a través de software xDriver LNS.

Desventajas:

- Las aplicaciones cliente tienen que conectarse inicialmente con el servidor LNS cuando se lanzan las aplicaciones LNS.

- **Arquitectura cliente/servidor con gestión externa**

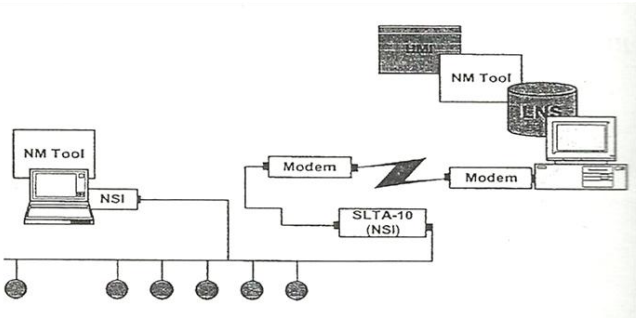


Figura. 1.17. Arquitectura cliente/servidor con gestión externa

Consta de un módem remoto que conecta una estación de trabajo operadora, que contiene el servidor de red, una herramienta de gestión de red y un HMI. Además cuenta con un PC cliente conectado localmente que tiene una herramienta de gestión de red en paralelo.

Ventajas:

- El servidor LNS puede ser mantenido desde el exterior de la red.
- No se necesita ningún PC conectado localmente a la red.
- El sistema puede estar configurado para marcar y responder automáticamente.

Desventajas:

- Se requiere un dispositivo de interfaz de red y un software para comunicación remota adicionales.

- Las actuaciones están limitadas por la disponibilidad de la conexión telefónica.

- **Redes sobre LAN o WAN**

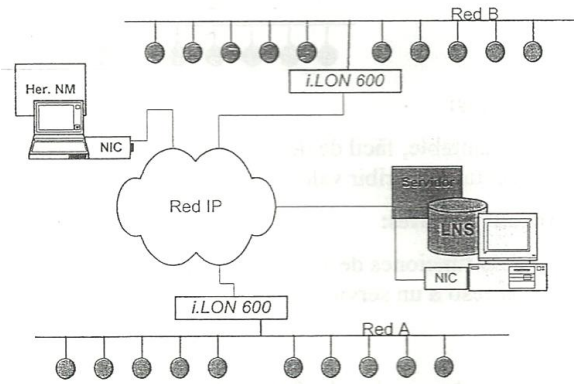


Figura. 1.18. Redes LAN o WAN

El tráfico entre los dispositivos y las herramientas de red es enrutado a través de una LAN o una WAN.

Un servidor Lonworks/IP i.LON 600 enruta los dispositivos de una red A, a los dispositivos de una red B usando un canal Backbone IP. Las herramientas cliente actúan como clientes completos “full clientes”.

Ventajas:

- Se pueden unir varias redes remotas para que formen parte del mismo dominio de red mediante el uso de redes IP existentes.
- Todas las herramientas remotas pueden operar como clientes completos remotamente sobre IP y el Servidor LNS también puede ser mantenido desde el exterior.

Desventajas:

- El software de configuración del servidor debe estar ejecutándose para realizar sincronización temporal se si está enrutando paquetes a través de redes WAN.

- **Cliente basado en navegador de web simple**

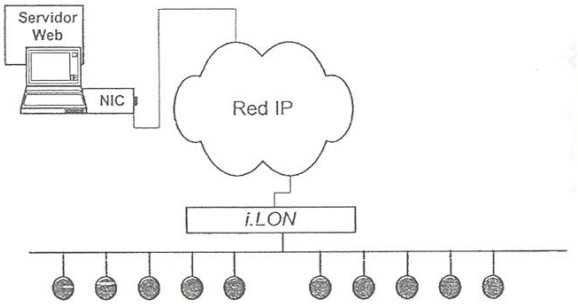


Figura. 1.19. Navegador web simple

Realiza tareas de monitorización y de control. Un navegador web estándar realiza peticiones de páginas web HTML estándar desde i.LON 100 ó i.LON 600. Las funciones avanzadas están provistas de interfaces Java Script, XML, DHTML y SOAP para sistemas de empresas.

Ventajas:

- Adaptable, fácil de desarrollar, y simple para usar con HMI que puede representar ó escribir valores de variable de red en formatos gráficos ó de texto.

Desventajas:

- Las funciones de administración de red no pueden ser desarrolladas sin acceso a un servidor LNS.

- **Sistema basado en web global**

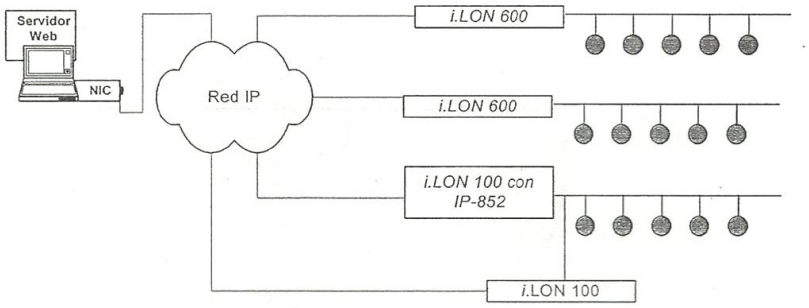


Figura. 1.20. Navegador web global

Los servidores Lonworks/IP i.LON 600 y el servidor internet i.LON 100 con opción de router IP-852 permiten la comunicación entre todos los dispositivos dentro de una gran red global, incluyendo conexiones virtuales de variables de red. El servidor de internet i.LON 100 provee aplicaciones basadas en web adicionales, tales como programaciones horarias y registro de eventos para una red global.

Ventajas:

- Adaptable, fácil de desarrollar, y simple para usar con HMI que puede representar ó escribir valores de variable de red en formatos gráficos ó de texto.
- Permite conexión virtual de variables de red sobre IP.

Desventajas:

- Las funciones de gestión de red no pueden ser desarrolladas sin accesos a un servidor LNS, que podría estar añadido a la arquitectura.

1.3.7. Topologías de red

1.3.7.1. Topologías físicas

El medio físico del canal de comunicación define la topología de red. El canal y el tipo de transceptor definen las características de cada topología de red.

- **Topología bus**

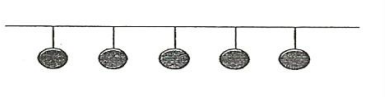


Figura. 1.21. Topología bus

Es un medio físico del canal de comunicación que incluye un inicio y un final de red definidos y diferentes. Tanto en el inicio como en el final de la red se debe tener una terminación de red.

Ventajas:

- Se pueden implementar cableados de dispositivo a dispositivo ó pequeñas ramificaciones.

Desventajas:

- Las ampliaciones son complicadas cuando se requieren incorporar nuevos dispositivos.

- **Topología libre**

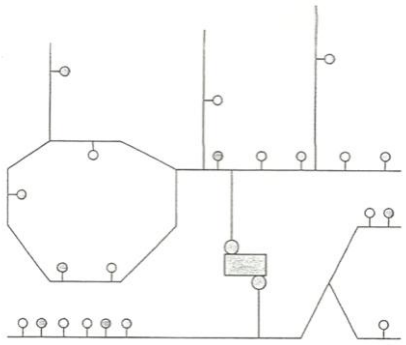


Figura. 1.22. Topología libre

Es una topología flexible en la estructura de cableado del canal de comunicaciones, pueden tener configuraciones tipo anillo, estrella, lazo ó una combinación de los tipos mencionados. Una terminación de red es necesaria en algún lugar del segmento; el lugar donde más se lo ubica es cerca del router.

Ventajas:

- Fácil de ampliar.
- Puede tener grandes ramificaciones hacia dispositivos y herramientas.
- Se pueden conectar nodos en cualquier lugar del canal.

Desventajas:

- Difícil de localizar.
- Se puede exceder los límites de capacidad del medio fácilmente.

- **Topología troncal "Backbone"**

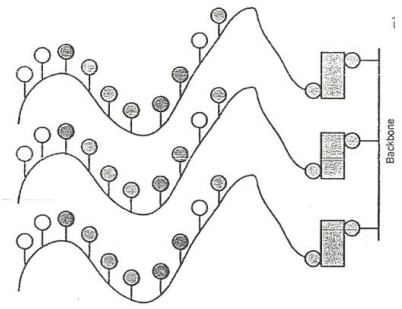


Figura. 1.23. Topología Backbone

Los dispositivos de distintos canales a un canal troncal común se conectan a través de los routers. Donde el canal troncal tiene una velocidad mayor, como un par trenzado de alta velocidad (XF1250) ó IP.

Ventajas:

- Reduce tráfico innecesario aislando el tráfico de los subsistemas.

Desventajas:

- Pueden haber limitaciones en la longitud del cableado del canal troncal.

1.3.7.2. Topologías lógicas

Se trata de un agrupamiento lógico y la estructuración del diseño de red. Se crean subsistemas que son sub áreas agrupadas e identificadas; cuyas sub áreas están formadas por dispositivos o bloques funcionales, que cumplen con una función de control en común o se encuentran en un área común.

Funciones de un subsistema

- Definible.
- Comprobable mediante pruebas de funcionamiento.
- Mediable.
- Demostrable.

Un subsistema tiene una interfaz limitada y definida; las operaciones más relevantes son realizadas de manera local en el subsistema.

Un subsistema está contenido en un único canal; aunque varios subsistemas pueden compartir un mismo canal, y se conecta a un canal a través de un router de subsistema.

Varios dispositivos pueden formar parte de varios subsistemas: Como por ejemplo: Subsistema de planta 1, Subsistema de planta 2; ó Subsistema de calefacción, Subsistema de control de accesos.

Cada subsistema de una red debe contener toda la documentación de sus características y de las funciones que este cumple, para así poder comprender de una manera fácil su funcionamiento y las secuencias de operaciones que este realiza.

1.3.8. Medios de transmisión de la red

El protocolo europeo ANSI/EIA 709.1, con norma ISO - 14908 es independiente de los medios de transmisión. El medio físico se caracteriza por el tipo de transceptor de los dispositivos.

Se puede elegir el medio que se ajuste a la aplicación, como por ejemplo una red Lonworks puede funcionar con cualquier red que use un transceptor Lonworks. El par trenzado es el más utilizado en redes Lonworks.

- **Tipos de medios de transmisión**

NOMBRE	NÚMERO/PARTE	DESCRIPCIÓN
Par trenzado	TP/FT-10	Canal de 78kbps usando cableado específico. Soporta topología libre.
	RS485	Topología Bus
	TP/XF-1250	Par trenzado de gran velocidad, canal de 1.25 Mbps usando cableado específico en topología Bus, comúnmente usado como troncal (Backbone).
Powerline (par tenzado)	TP/LPT-10 PLT-21 PLT-22	• 5kbps, 20 paquetes por segundo. • Portadora de frecuencia dual. • Provee alimentación a las aplicaciones de los dispositivos en los conductores de la comunicación. • Requiere una fuente acoplada regulada. • Es compatible con canales de par trenzado.
Radio frecuencia	RF-10	El canal de Radio frecuencia comunicación inalámbrica. • Puede alcanzar grandes distancias. • Puede requerir cableado in situ.

Fibra óptica	FO-10	Canal a 1.25 Mbps, usando fibra óptica, comúnmente utilizada para troncales y conexiones de gran distancia. Robusta en entornos ruidosos o pocos seguros.
IP-852	10/100 base T Ethernet	Se pueden hacer empaquetados Lonworks en paquetes UDP/IP. • Puede alcanzar grandes distancias. • Alta velocidad. • Opciones flexibles de conectividad.

Tabla. 1.1. Medios de transmisión[8]

[8] ECHELON, Corporation, ***Guía de Diseño de Redes Lonworks,*** Version 2.1.3, Impreso en España 2007, 200 páginas.

- **Tipos de canales comunes Lonworks**

	TP/FT-10	TP/LP-10	TP/XF-1250	PLT-22	Lonworks IP	FO-10
Sobrenombre	Topología Libre	Link Power	1250	Línea de potencia (powerline)	N/A	Fibra
Uso típico	“Última milla”	“Última milla”	Troncal	“Última milla”	Troncal	Troncal
Velocidad de transmisión	78kbps	78kbps	1.25Mbps	5.4kbps Banda-C 3.6kbps Banda-A	N/A	Cercano a TP/ XF-1250
Paquetes por segundo	144/168	144/168	747/835	14 (normalmente)	>5000 pkts/s	Cercano a TP/ XF-1250
Pico del tráfico	180/210	180/210	933/1043	20 (Protocolo CENELEC deshabilitado) 18 (protocolo CENELEC habililatdo)	?	Cercano a TP/ XF-1250
Topología	Libre, Bus	Libre, Bus	Bus	Libre, Bus	Libre	Bus
Soporte de repetidor en capa Física	Sí	Sí	No	No	Sí, en el sentido de un hub Ethernet	Sí

Terminación	Sí, uno por segundo (topología libre), o dos por segmento (topología bus)	Sí, uno por segundo (topología libre), o dos por segmento (topología bus)	Ambos extremos	Solo en aplicaciones especiales (por ejemplo transporte largos ó redes poco alimentadas eléctricamente)	Estándar Ethernet	N/A
Tipo de terminación	Tipo A o B	Tipo A o B	Tipo C	Personalizado	Estándar Ethernet (hub)	N/A
Tipos de cable[b]	CAT-5 Level IV Belden 8471 Belden 85102 JY (st) 2x2x0.8	Ver TP/FT-10, pero con la distribución eléctrica para ser tomada en cuenta	TIA 568A CAT-5 Level IV	N/A	CAT-5 (10Base-T, 100Base-F), RG58 (coax), etc	N/A
Máxima longitud Total de Cable[b]	2700 m (bus) 500 m (free)	2200 m (bus) 500 m (free)	130 m	Dependiente del ambiente	Ilimitado (a nivel mundial: Internet ó Local: LAN)	30 km
Máxima Longitud de la ramificación	Bus: 3 m	Bus: 3 m	0.3 m	N/A	N/A	N/A

Mínima distancia entre dispositivos	0	0	No más de 8 transceptores por 16 m de cable	N/A	N/A	N/A
Máxima distancia entre dispositivos	Libre: 500 m	Libre: 500 m	130 m	N/A	N/A	N/A
Número máximo de dispositivos por segmentos	64	128	64	N/A	N/A	Cientos

Tabla. 1.2. Canales comunes Lonworks[9]

[9] ECHELON, Corporation, ***Guía de Diseño de Redes Lonworks,*** Version 2.1.3, Impreso en España 2007, 200 páginas.

1.3.9. Canales de transmisión

- **Características a considerar en un canal de transmisión**

- Capacidad de ancho de banda.
- Distancia máxima del segmento.
- Topologías soportadas.
- Número máximo de dispositivos por segmento

    - La mayoría de los tipos de canales tienen restricciones en el número de dispositivos que pueden soportar.

- Número máximo de paquetes por segundo.

    - La tasa de transferencia está sujeto a muchos factores que pueden influir y variar la tasa de transferencia.

- Tipo de cable.
- Medios privados ó compartidos

    - Medios privado quiere decir que la comunicación no es compartida con otras partes.
    - Medios compartidos pueden ser compartidos con otras funciones; importante el alcance de los paquetes de red.

- Requerimientos de terminaciones

    - Muchos canales requieren una terminación explícita; que reduce las reflexiones y otros problemas que puede causar problemas en los paquetes.

- Herramientas de prueba y verificación disponibles.

- **Distintos tipos de canales**

a. IP-852 (Lonworks/IP)

Disponibilidad: Familia de productos Echelon i.LON, LNS y terceros

Funcionamiento típico: > 5000 pkts/s

Alcance típico: A nivel mundial (Internet) ó local (LAN)

Aspectos económicos: El valor varía dependiendo si existe ya o no una red instalada previa.

Características: Utiliza cualquier red IP como medio, cumpliendo las guías Lonmark para el ruteo IP, el empaquetamiento y la agregación.

Extender el alcance: Con una red LAN se puede conectar al internet y así al mundo, a través de líneas permanentes dedicadas (ADSL con IP fija) o mediante conexiones de teléfono con módems de internet apropiados. El Echelon i.LON 600 incluye la funcionalidad de soportar la RTC (conexión telefónica) en ambos sentidos de la conexión.

b. Radio frecuencia

Disponibilidad: Transceptores estándar (RF-10) y tipos no estandarizados.

Funcionamiento típico: 20 paquetes por segundo (RF-10), sujeto a la implementación del transceptor.

Alcance típico: Hasta algunos kilómetros, sujeto a la implementación del transceptor y a la potencia del transmisor.

Aspectos económicos: Transceptores relativamente costosos.

Características: Transceptores Half Duplex, es decir la transmisión y recepción no es simultánea, existe una diferencia de milisegundos lo cual causa una respuesta larga y pesada, y retrasos en el canal.

Extender el alcance: Es difícil a menos que se altere las frecuencias portadoras. Sin esta precaución, algunos paquetes duplicados provocarán tráfico extra al momento de ser vistos por el lado del receptor. Los repetidores RF actúan como repetidores de almacén y avance (S&F), es decir amabas mitades del repetidor compartirán un transceptor (half duplex). Así se ofrecen repetidores más baratos a consecuencia de mucho retraso del canal.

c. Fibra óptica

Disponibilidad: Transceptores estándar (FO-10) y modelos no estandarizados.

Funcionamiento típico: Comparable con TP/XF-1250.

Alcance típico: Hasta 30 km.

Aspectos económicos: Herramientas especializadas y entrenamiento necesario para acondicionar y conectar la fibra.

Características: Tiene alto número de dispositivos conectados, con pocas restricciones prácticas en la longitud del cable y dispositivos conectados. Se permite topología bus sin latiguillos, y no se permite topología libre. Insensible a interferencias electromagnéticas.

Extender el alcance: Se puede utilizar un router Lonworks con un transceptor de fibra óptica. Además se usa técnicas de repetición en capa física para acondicionar la señal.

1.3.10. Interfaces de red - Cómo las herramientas LNS se comunican con los dispositivos

Existen herramientas de administración de red LNS que se conectan desde un ordenador a una red Lonworks, mediante interfaces de red o llamados también adaptadores Lontalk.

Dichas interfaces pueden conectarse con casi todas las PCs, tipos de transceptores y configuraciones de bus. Al seleccionar una interfaz, se debe tomar en cuenta que debe soportar descargar imágenes de firmaware para la actualización de los dispositivos, y también que soporte firmware NSI para aplicaciones LNS.

- **Interfaces Lonworks para operación a nivel local:**

Protocolo	Interfaz de red	Empaque-miento	Interfaz del terminal	Atributos clave
Interfaz de Red USB U10/U20	U10: TP/FT-10 U20: PL-20	Adaptador USB PC	USB 2.0 (Compatible con USB 1.1)	Drivers Plug-and-Play para Windows XP, 2000 y Server 2003.
Tarjeta PCC-10 PCa	TP/FT-10 Empotrado, ranuras opcionales para TP/XF-78 y TP/XF-1250	Tarjeta de PC tipo II	Tarjeta de PC (anteriormente PCM-CIA)	Soporte Plug-and-Play

Adaptador LonTalk PCLTA-10 para PC	TP/FT-10, TP/XF-78, TP/XF-1250	Tarjeta de PC suplementa-ria	Tarjeta ISA de mitad de longitud	Memoria descargable, Plug-and-Play, Soporte NSI
Adaptador PCI Lontalk PCLTA-20	TP/FT-10, TP/XF-78, TP/XF-1250, TP-RS485, SMX	Tarjeta de PC suplementa-ria	Tarjeta PCI de mitad de longitud	Memoria descargable, Plug-and-Play, Soporte NSI

Tabla. 1.3. Interfaces Lonworks a nivel local[10]

- **Interfaces Lonworks para operación remota**

Protocolo	Interfaz de red	Empaque-miento	Interfaz del terminal	Atributos clave
SLTA-10 Empaquetado Adaptador EIA-232-a-Lontalk	TP/FT-10, TP/SF-78, TP/SF-1250, TP-RS485	Montura de pared/escritorio con fuente de alimentación 9-30 V CA o CD	EIA-232	Configuración DIP Switch; terminal cableado y atornillado; soporte NSI; ranuras de montaje con hoyos clave; conexión a módem o directa
PL-SLTA-10 Empaquetado Adaptador EIA-232-a-Lontalk	PLT-22	Montura de escritorio con entrada de corriente de 100-240 V CA	EIA-232	Configuración DIP Switch, fuente de alimentación; soporte NSI; conexión a módem o directa

[10] ECHELON, Corporation, ***Guía de Diseño de Redes Lonworks,*** Version 2.1.3, Impreso en España 2007, 200 páginas.

i.LON 10	TCP, TP/FT 10, PL-20	Adaptador Ethernet	Ethernet 10 Mbps	
i.LON 100	TCP, TP/FT-10, PL-20	DIN, Caja 8U	Ethernet 10/100 Base-T	Programación incorporada, registro de datos, manejo de las alarmas de las aplicaciones; entradas y salidas incorporadas; módems Dial in/out incorporados; interfaces de servicio Web SOAP/XML; notificación por correo electrónico
i.LON 100	TP/FT-10, TP/XF-1250	DIN, Caja 8U	Ethernet 10/100 Base-T	Convierte cualquier canal IP en un canal Lonworks

Tabla. 1.4. Interfaces Lonworks para operación remota[11]

[11] ECHELON, Corporation, ***Guía de Diseño de Redes Lonworks,*** Version 2.1.3, Impreso en España 2007, 200 páginas.

1.3.11. Routers y repetidores

- **Routers**

Uso

- Segmentar ó aislar tráfico.
- Construir redes extensas.
- Conectar medios físicos diferentes ó transceptores diferentes.
- Extender el largo del canal ó maximizar el número de dispositivos

Modos de configuración

- **Configurado**

En este modo tiene tablas de ruteo que definen las ubicaciones de las subredes y grupos para que el router pueda seleccionar a donde se dirigirán los paquetes.

- **Bridge**

En este modo el router solo reenvía paquetes solo en un dominio específico.

- **Aprendizaje**

En este modo el router va aprendiendo las ubicaciones de las subredes para reenviar los paquetes selectivamente.

- **Repetidor lógico**

En este modo el router reenvía todos los paquetes contenidos en un CRC válido “cyclical redundancy check”.

- **Repetidor de capa física**

Se lo usa para extender la longitud del canal y maximizar el número de dispositivos en el mismo.

Un repetidor puede:

- Reenviar todo, incluso ruido.
- Puede conectar cables ó medio diferentes.
- Puede causar tráfico excesivo en el canal cuando se utiliza mal.
- Es generalmente más barato que un router.

- **Comparación router y repetidor**

	Router	**Repetidor**
Análogo ethernet	Router	Hub
Capa OSI	3	1
Tipo de transceptor	Cualquiera	TP/FT-10, TP/LP-10
Número máximo en serie	Virtualmente ilimitado[a]	1
Puertos	2	Ilimitados (Típicamente <=8)
Fuente de Alimentación	Sí	Sí (a excepción de las alimentaciones por la red)
Instalación lógica	Requerida	No requerida

Retraso típico (TP/FT-10)	3-4 ms (sin incluir la cola para acceder al medio)	60 us (típicamente)
Buffer Local	Sí	No
Transparente a colisiones	No	Sí
Transparente a ruidos	No	Sí
Transparente a paquetes defectuoso	No	Sí
Filtrado de paquetes	Sí	No

Tabla. 1.5. Comparación router y repetidor[12]

a. El número máximo de paquetes en serie está determinado por el número máximo del timer de transmisión (3072ms) y la suma de los retrasos del canal y del router. En un diseño deben existir un número máximo de routers en fila, a pesar de ello es virtualmente ilimitado.

- **Comparación modos de configuración router**

	Repetidor	**Bridge**	**Aprendizaje**	**Configurado**
Validación de paquete	Sí	Sí	Sí	Sí
Filtrado de paquete	No	Dominio	Dominio, Subred, Grupo	Dominio, Subred, Grupo
Transparente a mensajes del Pin de Servicio	Siempre	Siempre	Siempre, si no está dada la subred	Siempre, si no está dada la subred
Configuración	N/A	N/A	Automática después de cualquier reset	A través de herramientas de administración de red

[12] ECHELON, Corporation, ***Guía de Diseño de Redes Lonworks,*** Version 2.1.3, Impreso en España 2007, 200 páginas.

Configuraciones redundantes	No	No	No	Posible
Misma subred en ambos lados	Posible[a]	Posible[a]	No permitido	No permitido

Tabla. 1.6. Modos de configuración router[13]

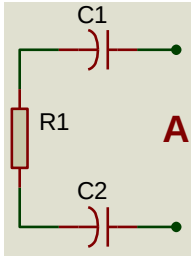
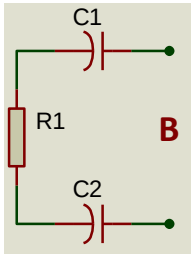
a. Previene de cambios a futuros a diferentes tipos de router

[13] ECHELON, Corporation, ***Guía de Diseño de Redes Lonworks,*** Version 2.1.3, Impreso en España 2007, 200 páginas.

1.3.12. Distintos componentes de infraestructura

- **Terminaciones de cable**

La terminación se la elige de acuerdo al canal y la topología que se use; de esta manera se asegura una comunicación buena y confiable.

Tipo de transceptor	Esquemas de la terminación	R1	R2	R3	C1	C2	Notas	# de Parte de Echelon
Topología Libre (TP/FT-10, TP/LP-10)		52.3Ω ±1%, 1/8W			100 Uf, ≥50V	100 Uf, ≥50V	Una terminación sencilla por cada canal de topología libre en cualquier localización	44100
Topología Bus (TP/FT-10, TP/LP-10)		105Ω ±1%, 1/8W			100 Uf, ≥50V	100 Uf, ≥50V	Una terminación a cada final del bus por cada canal de topología Bus	44101

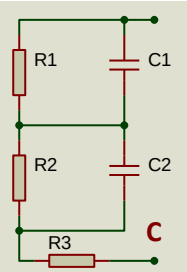
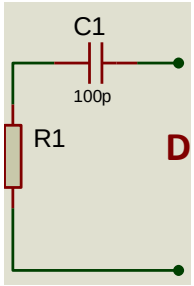
Topología Bus (TP/XF-78, TP/XF-1250)		59Ω ±1%, 1/8W	340Ω ±1%, 1/8W	102Ω ±1%, 1/8W	0.15 Uf, ≥50V metal poliéster	0.33 Uf, ≥50V metal poliéster	Una terminación a cada final del bus por cada canal de topología bus	44200
Tipos de Transceptores de Línea de Potencia (Power Line)		100Ω ±5%, 1/4W			0.47 Uf, ±1%, no-polarizado		Una terminación a cada final del bus por cada canal de topología Bus. Sólo es requerido para redes pocas cargadas o medios sin alimentación	N/A

Tabla. 1.7. Terminaciones de cables[14]

[14] ECHELON, Corporation, ***Guía de Diseño de Redes Lonworks,*** Version 2.1.3, Impreso en España 2007, 200 páginas.

- **Puesta a tierra del cable apantallado**

Cuando se usa par trenzado apantallado, debe conectar la terminación de acuerdo a la tabla en la sección anterior; y aterrar el cable por lo menos una vez por segmento y preferiblemente a cada dispositivo.

Tipo de transceptor	Rb	Cc	# de parte de Echelon
Todos	470 kΩ, 1/4W, ±5%	0.1 uF, 10% Poliéster Metalizado, ≥ 100V	N/A

Tabla. 1.8. Puesta a tierra de cable apantallado[15]

- **Acopladores de fase**

Como se conoce en un sistema que usa Power Line, es necesario el uso de este tipo de acopladores para:

- Comunicación entre transformadores.
- Monitorización y control de las tres fases usando la arquitectura Maestro/Esclavo.
- Comunicación Punto-a-Punto de las tres fases.

- **Fuentes de alimentación**

Estás suelen ser requeridas para canales con alimentación en la comunicación (Link Power TP/LP-10). Se usa generalmente una fuente de alimentación estándar 48 a 56 VDC y de 0 a 1.5 A, y un módulo de Interfaz Link Power LPI-10, que provee alimentación de Link Power de 41.0 a 42.4 VDC.

[15] ECHELON, Corporation, ***Guía de Diseño de Redes Lonworks,*** Version 2.1.3, Impreso en España 2007, 200 páginas.

1.4. PROGRAMACIÓN DE LA RED

1.4.1. Introducción

- **Proceso de diseño de la red**

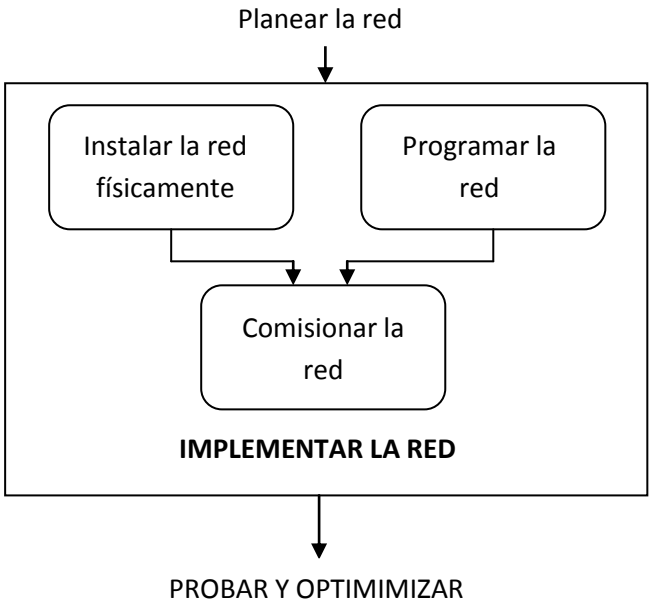


Figura. 1.24. Diseño de red

- **Programación de control tradicional**

Se escriben líneas de código utilizando plantillas pre-configurados. Características:

- Puede ser difícil de cambiar.
- Puede requerir un panel de control offline mientras se modifica.
- Es típicamente propietaria.
- Usualmente requiere una formación especial.

- **Programación Lonworks**

Es una programación orientada a objetos, con herramientas estándar; con objetos gráficos como bloques funcionales y conexiones de variables de red. Esta permite:

- Realizar modificaciones sin afectar en el funcionamiento de la red.
- No se necesita un controlador de final de cabeza “head end controller”, la programación la realiza a nivel del dispositivo con herramientas de administración de red estándares.
- Configuración simple de dispositivos usando Plug-ins de múltiples fabricantes basados en LNS.

1.4.2. Bloques funcionales

- **Tipos de representaciones**

Puntos de entrada/salida

- Sensores – analógicos ó digitales
- Actuadores – analógicos ó digitales

Controladores

- Aplicaciones específicas – VAV, control unitario, sensores de ocupación, etc.
- Aplicaciones Genéricas – PID, encoders, comparación analógica.

Controladores distribuidos en el sistema

- Programador horario, reloj en tiempo real, máquina de estados.
- Dispositivos de tendencias y alarmas.
- Dispositivos de Web Services.

- **Bloques funcionales Lonmark**

Se los conoce como perfiles funcionales estándar, que están muy bien documentados y tienen definidos las variables de red y las propiedades de configuración. Estos bloques promueven el intercambio entre múltiples vendedores.

Bloque funcional del objeto nodo

Se debe incluir un bloque funcional del objeto nodo cuando se añade más de un bloque funcional en un dispositivo. El objeto nodo FB permite a la herramienta de administración de red controlar el comportamiento del dispositivo a través de comando estándares de administración de dispositivos:

- Test
- Habilitar/Deshabilitar
- Invalidar
- Online/Offline
- Reporte del estatus del dispositivo

1.4.3. Variables de red (NVs)

Son aquellas que están incluidos en la definición de los bloques funcionales, son los que envían y reciben los datos dinámicos entre los dispositivos y la herramienta de red.

- **Tipos de variables de red estándar (SNVTs)**

Son llamados los tipos de datos comunes que envían y reciben dispositivos, ayudando a la interoperabilidad. Existen más de 180 tipos definidos por Lonmark. Cada una de las variables de Red incluyen valor, enumerado y tipos de combinaciones.

Los archivos de ayuda de Lonmark están incluidos con las herramientas de red LNS estándar para definir el formato del documento, la estructura y el significado de los SNTVs.

- **Tipos de variables de red de usuario (UNVTs)**

Cuando las variables de red existentes no cumplen con las necesidades de un dispositivo, los diferentes fabricantes pueden definir sus propias variables de red; pero estas variables de red deben definirse de forma estándar para poder ser certificados por Lonmark.

Cada fabricante debe proveer archivos de recursos que documente el formato y la estructura de la UNVT para las herramientas de mantenimiento de red.

- **Conexión de variables de red**

La conexión de virtual de variables de red es de tipo seguro. Las variables de entrada de red deben estar ajustadas a las variables de salida en tipo y longitud para que puedan conectarse.

La documentación del dispositivo define:

- Dirección de variable de red (Entrada/Salida)
- ID
- Mensaje predefinido de tipo de servicio
- Asociación de bloque funcional

- **Ejemplos aleatorios de definiciones de tipos de variables estándar de red**

Nombre SNVT	# SNVT	Medida	Tipo de categoría	Tamaño del tipo	Estructura/rango válido
SNVT_str_asc	36	Cadena de caracteres	Estructura	31 bytes	typedef struct { unsigned char ascii[31]; // 0…30 chars } SNVT_str_asc;
SNVT_temp	39	Temperatura	Punto fijo escalar – long sin signo	2 bytes	-274 .. 6,279.5 degrees C (0.1 degrees C)
SNVT_count_f	51	Cuenta de eventos	Punto flotante escalar	4 bytes	-1E38 .. 1E38 counts
SNVT_density	100	Densidad	Punto fijo escalar – long sin signo	2 bytes	0 .. 32,767.5 kg/m3 (0.5 kg/m3)

SNVT_time_sec	107	Tiempo Transcurrido	Punto fijo escalar – long sin signo	2 bytes	0.0 .. 6553.4 sec (0.1 sec). El valor 0xFFFF representa un dato inválido
SNVT_override	97	Prevalecer	Enumeración escalar	1 byte	Override_tEnumeración

Tabla. 1.9. Variables estándar de red[16]

- **Tipo de override_tEnumeración**

Valor	Identificador	Notas
0	OV_RETAIN	Retiene el valor actual
1	OV_SPECIFIED	Va al nivel especificado
2	OV_DEFAULT	Va al nivel por defecto
0xFF	OV_NUL	Valor no disponible

- **Ejemplo de una definición completa: SNVT_Switch**

Número SNVT	95
Medida	Cambio “Switch”
Categoría del tipo	Estructura
Tamaño del tipo	2 bytes
Estructura	typedef struct { unsigned value; Signed state; } SNVT_switch

[16] ECHELON, Corporation, ***Guía de Diseño de Redes Lonworks,*** Version 2.1.3, Impreso en España 2007, 200 páginas.

Campo	Unidades	Rango Válido	Notas
Valor	Porcentaje de 8 bit	0 .. 100%	Intensidad como porcentaje a escala complete, resolución 0.5%
Estado	Estado	0 .. 1, 0xFF	0 significa apagado, 1 significa encendido, 0xFF significa indefinido

Tabla. 1.10. Ejemplos[17]

1.4.4. Propiedades de configuración (CPs)

Son valores que se configuran y definen el comportamiento del dispositivo. Las propiedades de configuración se guardan en la memoria no volátil del dispositivo.

Los CPs se pueden aplicar en:

- El dispositivo
- Un bloque Funcional
- Una variable de Red

- **Tipos de propiedades de configuración estándar (SCPTs)**

Lonmark define los tipos de propiedades de configuración estándar para representar maneras usuales de configurar dispositivos y para ayudar a la interoperabilidad. Existen más de 160 tipos actualmente definidos pos Lonmark.
Los archivos de ayuda de Lonmark están incluidos con la herramienta de red LNS estándar para documentar el formato, la estructura y el significado de los SCPTs.

[17] ECHELON, Corporation, ***Guía de Diseño de Redes Lonworks,*** Version 2.1.3, Impreso en España 2007, 200 páginas.

- **Tipos de propiedades de configuración de usuario (UCPTs)**

Cuando las propiedades de configuración estándar no satisfacen las necesidades de dispositivos de diferentes de fabricantes. Los cuales crean sus propias propiedades de configuración para sus dispositivos; pero dichas propiedades deben ser estándar para poder ser certificados por Lonmark.

El fabricante debe proveer los archivos de ayuda que documente el formato y la estructura del UNVTs para las herramientas de administración de red LNS.

- **Valores CP que afectan al funcionamiento del dispositivo**

Como se señaló los CPs afectan el comportamiento local de un dispositivo.

Algunos comportamientos son los siguientes:

- Límite superior
- Límite inferior
- Punto de ajuste
- Coeficiente PID
- Retraso
- Histéresis

- **Valores CP que afectan al funcionamiento de la red**

Existen algunos CPs que pueden variar el funcionamiento de la Red como es la frecuencia con que el dispositivo propaga los valores de variable de red a la red; para ello existen algunos CPs que permiten controlar esto como son:

- *Envío en delta "Send on delta"*

Define la cantidad mínima de cambio en el valor de una NV antes de que sea transmitida.

- *Regulador de salida de tramas "Throttle" SCPTminSndTime)*

Define el período mínimo de tiempo entre cada transmisión de una variable de red. Ayuda a evitar saturar la red de mensajes; pues controla de manera rápida el cambio de valores I/O.

En la siguiente figura se muestra la transmisión de una variable de red. Dicha variable se actualiza cada 50 ms. A pesar de que la entrada cambie la actualización se la hace en este período.

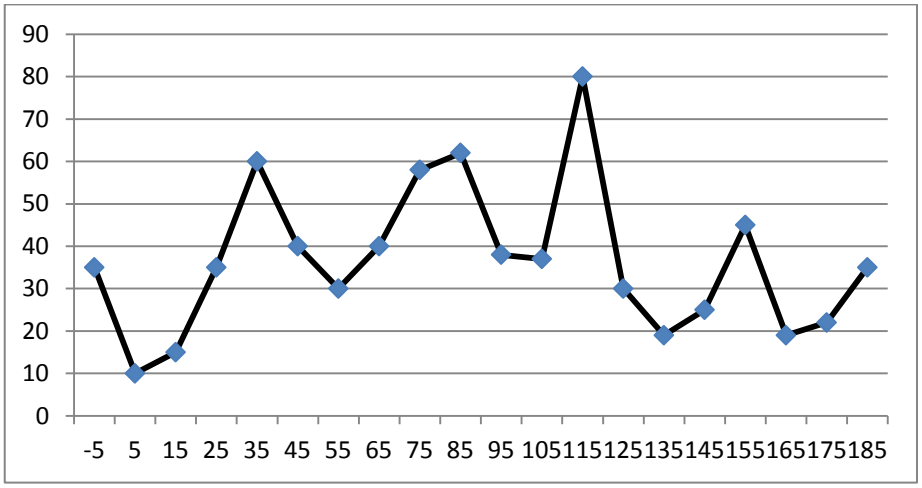


Figura. 1.25. Transmisión de una variable de red

- *Latido "Heartbeat" (SCPTmaxRcvTime)*

Controla el período máximo de tiempo antes de que el objeto automáticamente transmita su valor actual de la variable de red, aún cuando el valor no ha cambiado.

Esto permite una conexión a prueba de errores de los NVs. Si el dispositivo de recepción de trama falla al recibir y actualizar una variable NV en el intervalo de latido de recepción, el tiempo máximo de recepción (SCPTmaxRcvT), actúa con su valor de fábrica, se lo conoce como método de prueba de fallos.

El tiempo máximo de recepción debe ser de 4 veces superior al intervalo de tiempo de latido configurado en el dispositivo de envío. Si el tiempo máximo de recepción no está definido, los dispositivos de recepción de trama tendrán el último valor recibido en el evento antes de que se dé la falla en el dispositivo emisor de trama.

- **Algunos efectos de las propiedades de configuración**

- El latido determina el consumo mínimo de ancho de banda de una variable de red, aplica la siguiente fórmula:

$$\sum Z = \sum \frac{1}{H(s)} * P$$

Z = Es el consumo de ancho de banda (paquetes/segundo)
H = Es el latido en segundos
P = Es el número de paquetes enviados a la red por cada actualización

- Un regulador de salida de tramas es representado en milisegundos, la fórmula de consumo de ancho de banda es:

$$Z = \frac{1000}{T(ms)} * P$$

Z = Es el consumo de ancho de banda (paquetes/segundo)
T = Es el tiempo de apertura de la salida de tramas en milisegundos
P = Es el número de paquetes enviados a la red por cada actualización

Se debe lograr asignar el intervalo para que no se pierda ninguna actualización importante y el consumo de ancho de banda sea optimizado. El intervalo debe ser el más largo entre las actualizaciones de una salida de variable de red que sea compatible con el correcto funcionamiento del sistema.

- **Configuración de los plug-ins LNS del dispositivo**

Esta configuración es una aplicación cliente LNS, cuyos usos son:

- Aumentar la velocidad y simplificar la configuración del dispositivo

  - Guiar a los usuarios en tareas complejas.
  - Automatizar parte de las tareas de configuración.
  - Evitar las configuraciones no válidas ó poco seguras.

- Dar asistencia técnica a los dispositivos aislando y arreglando los errores del dispositivo.
- Proveer una interface hombre-máquina (HMI) para la monitorización específica del dispositivo y/o control.

- **Browser de plug-ins de dispositivos LNS**

Este browser es un Plug-ins que se utiliza cuando un fabricante no ofrezca una herramienta de configuración propietaria. El browser provee una vista de tablas de los NVs del dispositivo y los CPs que están incluidos en la documentación propia del mismo y le permite obtener y ajustar valores.

También presenta UNVTs y UCPTs en valores hexadecimales no ordenados cuando los archivos fuente no sean provistos a la herramienta de red, dificultando el ajuste.

- **Herramientas de configuración propietarias**

Estas herramientas pueden presentar algunos problemas como son:

- Incompatibilidad con la herramienta de administración de red LNS
- Requieren pagos de licencia de software
- Requieren entrenamiento especializado
- Los integradores prefieren herramientas estándar

1.4.5. Conexión de variables de red

Una conexión de red es un cable virtual que conecta una salida NV a una entrada NV. A esta conexión se la conoce como “Conexión virtual”.

Para lograr esta conexión se necesita una herramienta de administración, en este caso se tiene la herramienta de integración de Lonmaker que ayuda a crear conexiones así:

- Usando líneas para crearlas gráficamente.
- Usando números símbolos de conexión para definir el puerto y el destino de la conexión.

- **Tipos de conexiones**

- *Unicast:* Conexiones virtuales uno a uno.
- *Mutlicast:* Conexiones virtuales de uno a muchos o de muchos a uno. Conocidas como conexiones de cargabilidad de entrada y salida “fan-in, fan-out”.
- *Turnaround:* Son las conexiones de variables de red a sí mismas.

- **Unir los tipos de variables de red**

- Para las conexiones entre variables de red, ellas deben ser del mismo tipo.
- Las SNVTs deben ser del mismo tipo.
- Las UNVTs deben ser de la misma longitud.

Para agrupar diferentes tipos de variables de red existen traductores de bloques funcionales en los dispositivos LonPoint.

- **Tipo de servicio de mensajes**

Los servicios de mensajes definen como los mensajes son entregados y verificados.

Servicio de mensaje con reconocimiento "Acknowledgement"

En este servicio el dispositivo emisor espera una confirmación de reconocimiento "ACK" del dispositivo receptor para verificar la entrega.

Este servicio brinda robustez al envió de paquetes, aunque también ocasiona tráfico excesivo de mensajes, especialmente en conexiones grandes de multicast.

Número de paquetes por transacción en la red son:

- Dos paquetes en una conexión unicast exitosa.
- N+1 paquetes en una conexión multicast exitosa, donde "n" es el número de dispositivos receptores.
- Paquetes adicionales en caso de reintentos si no se recibe ningún ACK de los dispositivos receptores.

Servicio de mensaje de repetición/respuesta

En este servicio el dispositivo emisor pide un valor de variable de red al dispositivo receptor. Es así que como resultado da dos paquetes por cada transacción, adicionalmente a los paquetes por cada reintento si no se recibe respuesta del dispositivo receptor.

Servicios de mensaje sin reconocimiento

El dispositivo envía una única actualización NV y no espera respuesta del dispositivo receptor. Como consecuencia da un paquete por transacción sin importar el número de dispositivos receptores.

Servicio de mensajes repetidos

En este servicio el dispositivo emisor envía una serie de actualizaciones NV y no espera respuesta del dispositivo receptor. Este tipo de servicio con 3 mensajes repetidos tiene un 99% de tasa más exitosa que el servicio de reconocimiento.

- **Servicio de mensaje autentificado**

En este servicio el dispositivo receptor solicita al dispositivo emisor una verificación; produciendo así dos veces más tráfico que en un servicio de reconocimiento.

Este mecanismo tiene un número de transformación de 64 bits. Si la autenticación es usada existe una llave de autenticación de 48 bits usado por el dominio. Después de que la llave se carga en los dispositivos que utilizan la autenticación, el Neuron Chip protege la autenticación se ser pirateada. El uso de la autenticación para datos NV puede ser habilitada ó deshabilitada en base a las conexiones.

1.5. COMISIÓN DE DISPOSITIVOS LONWORKS

1.5.1. Introducción

- **El proceso de diseño de la red**

Una vez que se tiene ya instalada la parte física de la red y una red lógica en forma de programa de red; se pasa al proceso de comisionar que es aplicar la programación de la red a la red física, para poder realizar funciones.

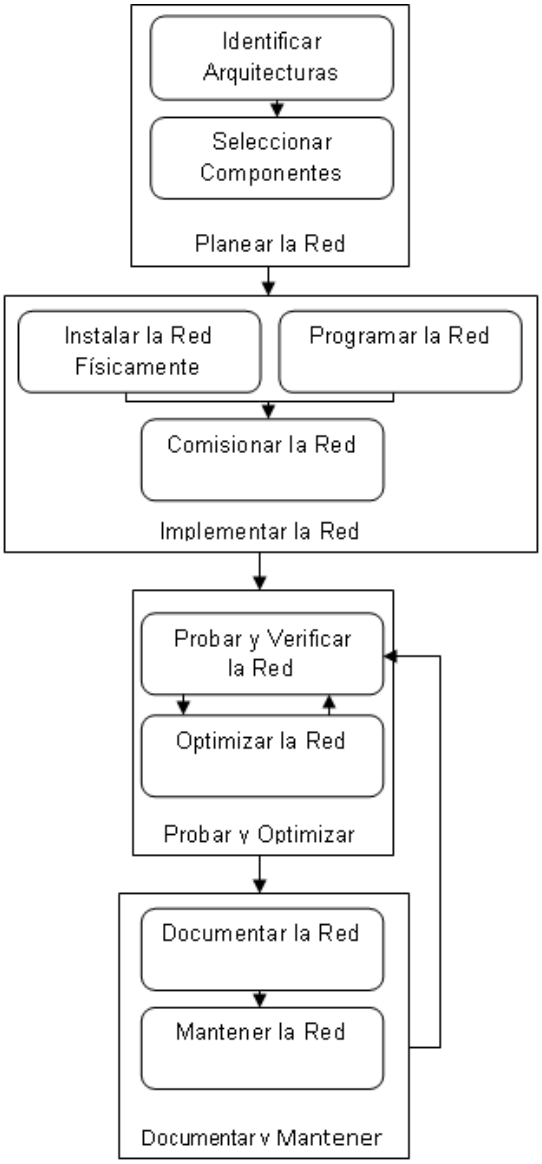


Figura. 1.26. Descripción para comisionar un nodo

- **Proceso para comisionar un dispositivo**

La herramienta de administración de red realiza el proceso de comisionar a través de la identificación del dispositivo por su ID del Neuron, asignándole su dirección subred/nodo, y descargando las definiciones de variables de conexión de red y los valores de las variables de configuración. Se pueden escoger como serán cargados los valores de configuración en el dispositivo:

- Valores actuales de la base de datos LNS.
- Valores de fábrica desde el archivo de interface del dispositivo (XIF) determinados por el fabricante.
- Los valores actuales del dispositivo. Se los usa cuando se configura desde una herramienta externa.

Para un router el comisionado es establecer las tablas de enrutamiento que indican la ubicación de la subred y grupo.

1.5.2. La ID del neuron del dispositivo

La ID del Nueron es el que permite identificar a un dispositivo, el cual está integrado en el Neuron Chip por le fabricante del Chip. Es un número de 48 bits
Si un dispositivo utiliza un procesador distinto al ID del Neuron ó Smart Transceiver, el protocolo ANSI/EIA 709.1 requiere que tenga un ID del Neuron ó un ID único de nodo integrado en el procesador.

La función “Wink” del administrador de red permite identificar físicamente el dispositivo que está comisionado, verificando que tiene el ID del Neuron correcto. Esto lo puede hacer tanto automática o manualmente.

- **Obtener el ID del neuron**

Manualmente o con lector de código de barras

Muchos fabricantes incluyen etiquetas con la ID del Neuron en código de barras o en texto, es así que se puede introducir el ID tecleándolo o escaneándolo. Este proceso se puede realizar mientras la herramienta de red está en el modo de diseño “engineered mode”, no en el modo conectado de red.

Para realizar esto se debe estar seguro de que el dispositivo será instalado físicamente donde esté indicado en el diseño de red.

Automáticamente presionando el pin de servicio

De esta manera se difunde el ID del Neuron y el ID del Programa “Program ID” a la red.

Cuando la herramienta de red pida el ID del Neuron del dispositivo, se puede presionar el pin de servicio del dispositivo correcto; esto es en el proceso de comisionado. Si el ID del dispositivo y el canal del dispositivo ha sido recibido de acuerdo al diseño de la red, entonces la herramienta de red realiza el comisionado.

Rápidamente mediante el descubrimiento del dispositivo

La herramienta de red encuentra dispositivos no configurados en la red y lo ajusta al diseño de la red. La herramienta de red envía un mensaje de administración solicitando los dispositivos desconocidos, es así que se relaciona los dispositivos descubiertos con su locación y su ID de programa. Necesario que la herramienta de red debe estar conectada en red.

1.5.3. Comisionar con la red conectada “Onnet” ó desconectada “Offnet”

Para comisionar un dispositivo y router, la herramienta de administración tendrá que:

- Verificar que le dispositivo físico tiene la misma interface que la definida en la base de datos LNS.
- Asignar la dirección lógica al dispositivo.
- Actualizar la tabla de direcciones del dispositivo.
- Descargar los valores de las propiedades de configuración.
- Actualizar las tablas de enrutado

- **Comisionar con la red desconectada “Offnet”**

En esta forma de comisionar todos los cambios de configuración de la red son aplicados a la base de datos LNS, y no a los dispositivos físicos. Dichos cambios de configuración de los dispositivos son verificados y puestos en cola para un proceso posterior, cuando se esté en estado “Onnet”. Se recomienda conectarse cuando el tráfico adicional de red tenga el menor impacto en la red.

A pesar de estar desconectada la herramienta de red, esta puede adquirir el ID Neuron, visualizar y probar el dispositivo.

- **Comisionar con la red conectada “Onnet”**

En esta forma la herramienta de red transmitirá todos los parámetros de diseño al mismo tiempo que se está comisionando, esto impacta al tráfico de red mientras la información es transmitida.

Con la red conectada el comisionado se realiza en serie; cada proceso de comisionado se debe ejecutar antes de que se ejecute el siguiente. Esto se lo

hace ya que puede afectar en el funcionamiento si múltiples herramientas clientes están intentando comisionar dispositivos al mismo tiempo.

1.5.4. Asuntos de comisionar

- **Comisionar routers**

Todos los routers deben ser comisionados al inicio del proceso, ya que para comisionar un dispositivo todos los routers entre dispositivos y la herramienta de red deben estar comisionados y en línea.

- **Poner los dispositivos en línea "Online"**

Se deben probar los dispositivos sensores y conectarlos a la línea antes que los actuadores para asegurar un buen funcionamiento de la red cuando se enciendan los dispositivos.

Se recomienda poner offline los dispositivos después de haber comisionado los dispositivos.

- **Minimizar el impacto del tráfico**

Se recomienda completar el diseño de la red antes de comisionar los dispositivos, de esta manera se minimiza el impacto en el tráfico de la red cuando se actualicen múltiples dispositivos y routers para ampliaciones, movimientos y cambios mientras la red está en funcionamiento.

Si se necesita realizar cambios cuando ya se ha comisionado, se puede minimizar el impacto del tráfico poniendo la herramienta de red fuera de línea mientras se hacen los cambios requeridos.

1.5.5. Reglas para comisionar

Regla 1: Los routers se deben comisionar en orden topológico desde el servidor LNS.

Regla 2: Para comisionar un dispositivo, todos los routers que están en la trayectoria del dispositivo deben ser configurados previamente.

Regla 3: El lado más cercano del router es el lado más cercano a la herramienta de administración de red en el momento de comisionado.

Regla 4: El comisionado es el último proceso del diseño.

1.6. ELEMENTOS FÍSICOS DEL SISTEMA DE CONTROL DE ACCESOS DE ISDE

1.6.1. Nodo lector de proximidad INP-120X

Previa la especificación física del nodo Lector de Proximidad, es importante conocer las funciones generales con las que este cumple:

- Control de acceso o iluminación si se detecta una tarjeta válida o no válida.
- Control de acceso a través de una validación de tarjeta incluida en la lista blanca.
- Flexible actualización de la lista blanca.
- Salidas indicadoras cuando una tarjeta es válida o no válida.

1.6.1.1. Características físicas

A continuación, se presenta la estructura física del nodo además de las conexiones que este puede tener, junto con las partes extras que este necesita para realizar lo mencionado.

1.6.1.2. Diagrama físico

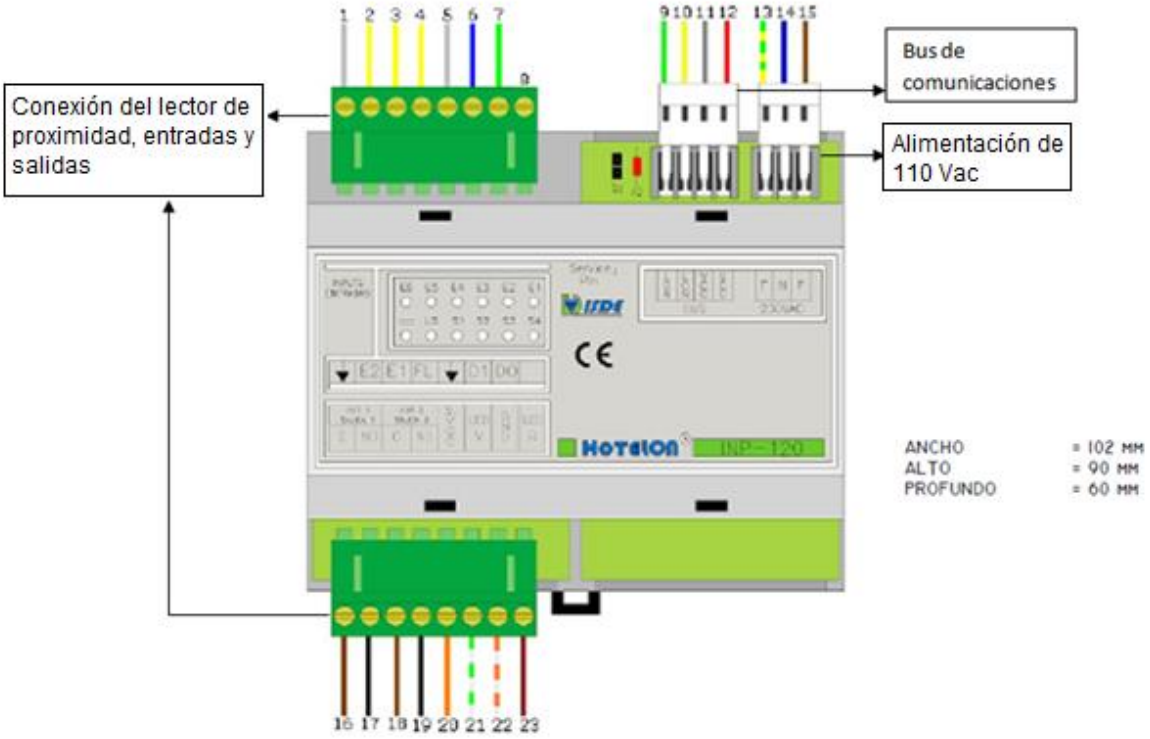


Figura. 1.27. Descripción física nodo INP-120

1.6.1.3. Bloques de conexión

Consta de las siguientes partes que están enumeradas de acuerdo al gráfico indicado anteriormente:

1.6.1.4. Conexión del lector de proximidad

Con lector de proximidad ILP-100/ILP-200

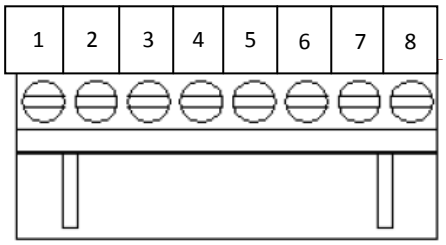


Figura. 1.28. Conector datos de lector y entradas

1 Común de las entradas 1 y 2

2 Entrada 2

3 Entrada 3

4 Salida de fin de lectura

5 GND

6 Dato 1 lector Wiegand

7 Dato 0 lector Wiegand

8 No se usa

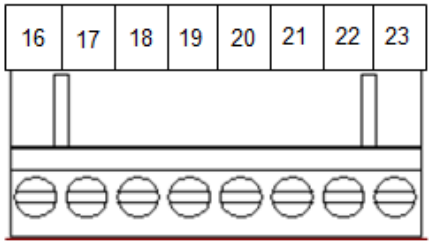


Figura. 1.29. Conector leds de lector y salidas

16 Fase circuito salida 1

17 Salida circuito 1

18 12 Vcc para cerradura

19 Salida a cerradura

20 Alimentación 12 Vcc al lector

21 Led verde o acceso permitido

22 Neutro lector Wiegand/Led

23 Led rojo o acceso denegado

1.6.1.5. Alimentación de 110 Vac

Los colores de los cables deben ser acordes a la RBT

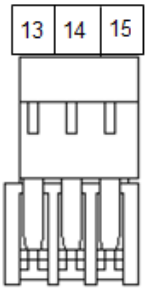


Figura. 1.30. Gráfico conector de alimentación AC

13 Tierra alimentación

14 Neutro alimentación 110 Vac

15 Fase alimentación 110 Vac

1.6.1.6. Bus de comunicación

El bus de comunicación sirve para la comunicación con otros nodos que pueden existir en una red Lonworks, las líneas de comunicación se conectan mediante cable (CCB-24) para el bus DOMOLON.

Las terminaciones de red deben ser: Modelo CTR-110; las cuales se las pone de acuerdo a la topología de red que se implemente en la determinada instalación.

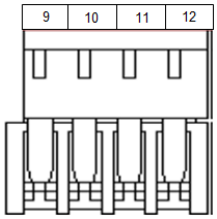


Figura. 1.31. Gráfico conector comunicación LON y alimentación 12 V

9 Comunicaciones LON

10 Comunicaciones LON

11 Alimentación 0Vcc

12 Alimentación 12Vcc

1.6.1.7. Conectores

Vista de conectores reales

Bus de comunicación

Figura. 1.32. Conector comunicación LON y alimentación 12V

Alimentación de 110 Vac

Figura. 1.33. Conector de alimentación AC

Conector de entradas y salidas

Figura. 1.34. Conector de entradas y salidas

1.6.1.8. Firmware

Es el software que se carga al nodo Lector de Proximidad, el cual contiene todas las variables y parámetros de configuración que el nodo tendrá disponible para una instalación. Dependiendo del nodo INP-120 que se use se usa una comunicación y Firmware diferente.

Modelo	Comunicación	Firmware
INP-120R	RS – 485	**XIF:** A131300000001.XIF **APB**: A131300000001.APB
INP-120F	FTT	**XIF:** F131300000001.XIF **APB:** F131300000001.APB

Tabla. 1.11. Tipos de nodos y firmware

1.6.1.9. Configuración del nodo INP-120[18]

El nodo INP-120, consta de ciertas variables de red y propiedades de configuración que se usan para la correcta programación y control del mismo.

1.6.2. Lector de proximidad ILP – 200

Figura. 1.35. Vista frontal lector

Figura. 1.36. Vista posterior lector

[18] Para mayor detalle de las variables de red y propiedades de configuración mirar el índice de Data sheets al final del documento.

Este dispositivo se lo puede utilizar tanto para el Nodo de control INP-120X como para el Nodo de control INH-551X, para el sistema DOMOLON y el sistema HOTELON, respectivamente.

Para poder trabajar con el lector de proximidad ILP-200 usando el Nodo de Control INP-120X, es necesario la correcta ubicación del jumper; tal como se muestra en la figura.

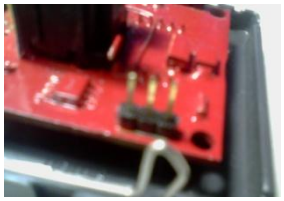


Figura. 1.37. Lector sin jumper

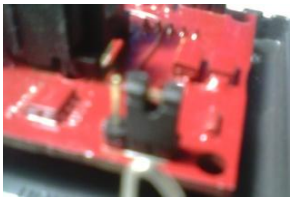


Figura. 1.38. Lector con jumper

1.6.2.1. Características[19]

- Usa la tecnología Wiegand 26 bits o ISO configurable por jumpers.
- Compatible con cualquier sistema de control de acceso.
- Dotado de dos diodos LED para indicar acceso válido o inválido.
- Diodo LED interno amarillo para indicar lectura de tarjeta.
- Cuerpo acabado en pizarra y marco gris como estética base.
- Estética configurable según proyecto.
- Rápida conexión por RJ45.
- Bajo coste y amplia gama de acabados.

[19] Para mayor detalle de su especificación funcional mirar el índice de Data sheets al final del documento.

1.6.3. Tarjetas de proximidad

Las tarjetas de proximidad son una gran opción al momento de elegir un sistema de control de accesos; ya que son buenas portadoras de información, además que su desgaste por rozamiento no existe y la duración es prácticamente indefinida. Son utilizadas generalmente en controles de accesos en eventos, peajes o transporte público. Para este tipo de sistemas se usa un rango de frecuencias bajas.

Estas tarjetas de proximidad utilizan un chip que trabaja a una frecuencia de 125 Khz con una rápida velocidad de lectura, con un alcance que varía desde 2 cms a 1 metro, dependiendo del lector que se use (para el lector ILP-200 es de 2 a 5 cms), también es capaz de almacenar hasta 1 Kb de información. Las tarjetas de baja frecuencia se suelen utilizar en servicios que no requieren más de un dato como el control de acceso al transporte público, dispensadores automáticos, máquinas de vending, etc.

- Chip sólo lectura: capacidad de 64 bits que alberga un ID único por cada tarjeta.
- Chip lectura/escritura: hasta 264 bits de memoria protegida por contraseña.

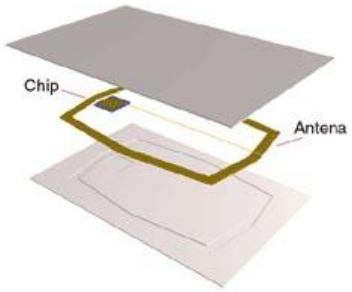


Figura. 1.39. Chip de baja frecuencia - 125 Khz

En la Figura. 1.39 se puede observar la estructura interna de una tarjeta de proximidad. La tarjeta consta de una antena que está en varios niveles (tres de 100-150 espiras cada uno) alrededor de un núcleo de ferrita. Mediante la

inducción electromagnética se produce el voltaje necesario para alimentar un circuito integrado utilizando un número suficiente de espiras. Y así cuando una tarjeta se aproxima al lector, este envía una onda por RF a la tarjeta la cual devuelve un código único. Dato que ingresa al sistema para ser procesado.

1.6.4. Interfaz de red USB (IAUSB-F)

Figura. 1.40. Interfaz de red USB (IAUSB-F)

Este dispositivo se lo puede utilizar tanto para el sistema DOMOLON y el sistema HOTELON.

1.6.4.1. Características[20]

- Interfaz de red LonWorks a USB de bajo coste.
- Soporta canal LonWorks de par trenzado (FTT-10) de topología libre.
- Rendimiento de procesamiento y funcionamiento más altos posible de la red.
- Diseño rugoso y conectores extraíbles.
- Auto instalación para Windows XP, 2000, NT y Server 2003.
- Compatible con aplicaciones OpenLDV y el Analizador de protocolo LonScanner.
- Fácil Instalación.

[20] Para mayor detalle de su especificación funcional mirar el índice de Data sheets al final del documento.

1.6.5. Otro elementos

Adicionalmente para el sistema físico de control de accesos se necesitará:

- El uso de un pulsador el cual servirá para poder salir de una puerta del recinto. Es importante recordar que el lector de proximidad es solo para el acceso a una puerta.
- El uso de un contacto magnético para detectar el estado de una puerta si está cerrada o abierta, dicho elemento irá conectado a una entrada del nodo INP-120.
- Y el uso de una cerradura, ya sea de pistillo o electromagnética; para poder accionarla y así abrir una puerta.

1.7. COMUNICACIÓN

1.7.1. Comunicación PC – nodo INP-120

La comunicación entre el PC y el dispositivo de control de accesos INP-120 es la parte esencial para poder comenzar con el diseño del software que permitirá obtener la interfaz de usuario deseada.

Mediante la comunicación entre PC y NODO se podrá enviar y recibir datos entre ellos, manipulando las Variables de Red y Propiedades de Configuración del NODO INP-120; con las cuales se podrá controlar y configurar al dispositivo/s mencionado desde la PC mediante un software amigable.

1.7.1.1. Protocolo de comunicación

Es importante mencionar antes de introducirse al protocolo de comunicación entre la PC y el NODO INP-120, que se debe diferenciar entre el protocolo de comunicación de una red Lonworks con el protocolo que se usará para conectarse a través de la PC a una red Lonworks.

a. Protocolo de comunicación DDE (Dynamic data exchange)

El protocolo DDE con su traducción en español es conocido como el intercambio dinámico de datos.

DDE es una agrupación de especificaciones para el intercambio de datos y control de flujo de información entre aplicaciones usando mensajes de Windows entre una aplicación Servidor y una aplicación Cliente.

- **Características de DDE**

1. DDE es asíncrona, el cliente programado envía mensajes de Windows para el servidor y lleva acabo el procesamiento; Windows mantiene el mensaje hasta que el servidor esté listo para recibirlo y procesarlo.
2. DDE es muy fácil de aplicar pero lo único que puede hacer es transmitir datos. Sólo se puede controlar a otra aplicación, ya que el destinatario pueda tratar los datos como un comando.
3. La esencia de DDE es que los clientes se conectan a un servidor que ya está corriendo.
4. Usando DDE para comunicarse entre componentes de una misma aplicación es posible pero no da beneficio ya que solo transmite datos nada más.
5. Es probable que sirva a una amplia gama de clientes, y puede ser actualizado sin necesidad de que todos ellos se vuelvan a compilar.
6. Es inmune a los problemas asociados con las diferentes versiones de las DLL del sistema en diferentes máquinas.
7. Puede ser pequeño y autónomo.
8. Los clientes no pueden interferir con el funcionamiento del servidor por ser lento u ocupado.
9. La aplicación que envía la información se le conoce como servidor y la aplicación que recibe la información es el cliente.

DDE es ideal para permitir que un programa monitoree a otro, ya que ningún programa se ejecuta en el contexto del otro; por lo tanto estos programas no interfieren entre ellos.

Algo importante de mencionar es que la aplicación servidor debe estar funcionando antes de que la aplicación cliente le pida la información. Si no es así, se generará un error.

Cuando se requiere una comunicación DDE Cliente – Servidor, el mensaje que envía el Cliente al Servidor que está corriendo en el PC se lo direcciona usando una dirección DDE que consta de tres partes: *Aplicación, Topic* e *Item.*

- **Aplicación:** El nombre del Servidor al cual se direcciona el mensaje, por ejemplo una Aplicación puede ser Excel o Visual Basic.
- **Topic:** Se asigna de acuerdo a la aplicación a la cual se direcciona, es el tipo de información que el Cliente está interesado en enviar o recibir; como por ejemplo en Excel, el Topic es la hoja de cálculo
- **Item:** Es la parte específica de información que el Cliente desea enviar o recibir, hacia o desde el Servidor; según sea el caso requerido; por ejemplo en Excel sería una celda específica.

Petición Cliente = Aplicación|Topic!Item

Como se menciono el protocolo DDE se usa para una comunicación entre aplicaciones de Windows, pero para poder realizar una comunicación entre un aplicación de Windows.

b. DDE en Visual Basic 6.0

El objetivo al que se quiere llegar en el presente trabajo es la comunicación entre una aplicación de Windows (Visual Basic 6.0) y un dispositivo remoto (NODO INP-120) mediante el protocolo DDE, y siendo este el caso DDE será analizado.

En Visual Basic 6.0 se pueden traspasar datos, mediante TextBox, Label, PictureBox, ComboBox.

A continuación se muestran las propiedades usadas por Visual Basic 6.0 para poder realizar una comunicación DDE Servidor – Cliente, las cuales serán explicados a continuación:

- Ejemplo de un TextBox para un enlace DDE de Lectura

```
Text1.LinkMode = 0
Text1.LinkTopic = "Project1|MyTopic"
Text1.LinkItem = "txtSource"
Text1.LinkTimeout = 100
Text1.LinkMode = vbLinkAutomatic
```

- **Propiedades:**

1. LinkMode

Este comando nos ayuda a realizar una comunicación DDE mediante un formulario o un control de Visual Basic como se señaló anteriormente (TextBox, Label, etc)

- *Formulario:*

Dicha configuración se la puede hacer dentro de las propiedades del formulario a comunicar.

0 = None	No puede existir comunicación DDE con el formulario.
1 = Source	El formulario permite que exista una comunicación DLL entre uno de sus controles y otra aplicación.

- *Control:*

Esta configuración es usada para la comunicación con un control de Visual Basic.

0 = None	No existe comunicación DDE con el control.
1 = Automático	Los datos se traspasarán desde la aplicación servidor al control de la aplicación cliente cada vez que cambie el dato en la aplicación servidor.
2 = Manual	Los datos se traspasarán cuando lo pida la aplicación cliente, mediante la orden *LinkRequest*.
3 = Notify	Cuando existe un cambio en los datos de la aplicación servidor, ésta notifica a la aplicación cliente que el dato ha cambiado, pero no le envía el dato nuevo. En el control de la aplicación cliente se genera el evento *LinkNotify*, en cuyo procedimiento podremos escribir el código necesario dependiendo de nuestra aplicación. Para traer la información, debe ejecutarse la orden *LinkRequest*.

2. LinkTopic

Esta propiedad es de lectura y escritura, tanto para los controles como para los formularios.

Cuando un control destino quiere establecer una comunicación DDE “llama” a la aplicación origen, y dentro de ella, al formulario que contiene el control cuya información se quiere transferir. A ese formulario se le llama por un nombre que le debemos poner al formulario en su propiedad *LinkTopic*. A este nombre se le denomina **Tema**.

- La propiedad *LinkTopic*, para un formulario de origen, devuelve o establece el **tema** al que el formulario “responde” en una conversación DDE.

Sintaxis *nombredelformulario.**LinkTopic** [= tema]*

- Para un control destino, La propiedad *LinkTopic* contiene el nombre de la aplicación y el tema, ambos separados mediante el carácter “|”.

Sintaxis *nombredelcontrol.**LinkTopic** [= aplicacionorigen|tema]*

El nombre de la aplicación origen será el nombre del proyecto de Visual Basic o la aplicación de o hacia donde se quiere transferir la información.

El tema será el mismo al que “responde” el formulario donde se encuentra el control que contiene la información a transferir; o el tema es el nombre del proyecto en el que se trabaja dentro de otra aplicación.

3. LinkItem

Esta propiedad solo tiene el control destino de la información. No la tiene el formulario origen. En esta propiedad deberá expresarse el nombre del ***control origen*** de la información.

Esta propiedad es de lectura y escritura; sirve para saber el nombre del control origen de los datos, como para establecerlo en tiempo de ejecución.

Sintaxis *objeto.LinkItem [= cadena]*

Donde *cadena* es el nombre del control origen que tiene los datos y *objeto* es el nombre del control en el cual se usa la propiedad *LinkItem*.

4. LinkTimeout

Esta propiedad devuelve o establece la cantidad de tiempo que un control espera una respuesta a un mensaje DDE.

Sintaxis *objeto.LinkTimeout [= número]*

Donde *número* es una expresión numérica que especifica el tiempo de espera en décimas de segundo. Se usa esta propiedad para ajustar el tiempo que un control destino espera la respuesta de una aplicación origen. Usando *LinkTimeout* se puede evitar la generación de un error por Visual Basic si una aplicación origen tarda mucho en responder.[21]

5. LinkNotify

Este evento ocurre cuando la propiedad LinkMode del control destino está establecido a 3.

Private Sub objeto_LinkNotify([índice As Integer])
End Sub

En este procedimiento se puede escribir el código necesario que se quiere que realice la aplicación con la notificación de que un dato ha cambiado.

[21] **Nota:** El plazo mayor de tiempo que un control puede esperar es 65.535 décimas de segundo, es decir, sobre 1 hora y 49 minutos. Al establecer *LinkTimeout* a 1 se indica al control que espere la respuesta en una conversación DDE durante el mayor plazo de tiempo. El usuario puede forzar que el control deje de esperar presionando la tecla ESC.

6. LinkRequest

Este evento pide a la aplicación origen de una conversación DDE que actualice el contenido de un control Label, PictureBox o TextBox.

Sintaxis *objeto.LinkRequest*

Siendo *objeto* el nombre del control destino de la aplicación. El destino debe entonces usar el método *LinkRequest* para actualizar los datos.

7. LinkSend

Esta propiedad transfiere el contenido de un control PictureBox a la aplicación destino de una conversación DDE.

Sintaxis *objeto.LinkSend*

Objeto debe ser un control PictureBox de un objeto Form que sea origen de una conversación DDE.

Cuando se establecen vínculos automáticos con un objeto Form de una aplicación, Visual Basic notifica cuando el contenido de un control TextBox o Label origen cambia. Pero, Visual Basic no notifica automáticamente a una aplicación destino DDE cuando el valor de la propiedad Picture de un control PictureBox origen cambia, ya que la imagen puede tener muchos datos. Por lo tanto Visual Basic requiere el uso del método **LinkSend** para notificar explícitamente a las aplicaciones destino DDE cuándo cambia el contenido de un control PictureBox.

8. LinkPoke

Transfiere el contenido de un control Label, PictureBox o TextBox a la aplicación origen de una conversación DDE.

Sintaxis *objeto.**LinkPoke***

Objeto es el nombre del control Label, PictureBox o TextBox involucrado en la conversación DDE como destino.

Si *objeto* es un control *Label*, *LinkPoke* transfiere el contenido de la propiedad *Caption* al origen. Si *objeto* es un control *PictureBox*, *LinkPoke* transfiere el contenido de la propiedad *Picture* al origen. Si objeto es un control *TextBox*, *LinkPoke* transfiere el contenido de la propiedad *Text* al origen.

LinkPoke también permite que un objeto destino suministre datos al origen; aunque no todas las aplicaciones origen aceptan información de esta forma.

1.7.1.2. LNSDDE Server 2.1

Una red Lonworks es instalada y puesta en marcha mediante una herramienta de manejo de red, como es el Software Lonmaker. Pero para poder tener un monitoreo y control de la red Lonworks se usa el Software LNSDDE Server 2.1, el cual es un Servidor para un servicio de una red de Lonworks mediante comunicación DDE.

a. Características del LNSDDE Server 2.1

Amplia capacidad de encuesta.- Cuando en una red Lonworks, se usa una interfaz rápida LNS conectada a un canal Lonworks; o una interfaz de red IP conectada a un canal Lonworks IP. Este programa es capaz de manejar hasta 1000 puntos simultáneamente.

Amplia capacidad de unión.- El programa tiene una tabla de direcciones con 32768 entradas, con lo cual le permita al LNSDDE Server PC ser un miembro de cada grupo sin dominio y soportando una alta tasa de conexiones.

Tiempo de ejecución LNS 3.- El rendimiento mejora como resultado de un mejor proceso a través del Tiempo de Ejecución LNS, la interfaz de red y el incremento de las dos capacidades mencionadas anteriormente.

Soporte del canal Lonworks/IP.- El LNSDDE Server puede ser usado también para monitorear y controlar a clientes remotos sobre un canal Lonworks/IP, sin requerir una tarjeta de interfaz de red LNS; lo cual ayuda al incremento del rendimiento. Así por ejemplo se puede manejar hasta 600 puntos por segundo y recibir hasta 1200 actualizaciones por segundo.

Soporte de suitelink Wonderware.- El procotolo Suitelink de Wonderware es ahora soportado por LNSDDE Server, además del protocolo DDE

Soporta múltiples redes.- El LNSDDE Server puede manejar hasta 100 redes LNS a través de una interfaz de red LNS simple, incluyendo redes locales y remotas. Este permite una aplicación DDE simple para proveer una interfaz a las múltiples redes a través de una interfaz de red simple, o a través de múltiples interfaces de red.

Controladores actualizados de red.- Incluye drivers para manejar tarjetas PPC-10, PCLTA-10, PCLTA-20; las cuales tienen un nuevo firmware que permite un mejor rendimiento de las aplicaciones LNSDDE Server.

Operación de modo de servicio.- Permite que el LNSDDE Server continúe trabajando aun como operador registrado o no registrado de Windows XP, Windows NT o Windows 2000. Cuando se corre como un servicio de sistema, el LNSDDE Server puede ser configurado para interactuar con el escritorio del usuario y que se puedan ver todos los puntos habilitados para el LNSDDE Server.

Aunque el LNSDDE Server se puede correr escondido para que el usuario no tenga acceso a este.

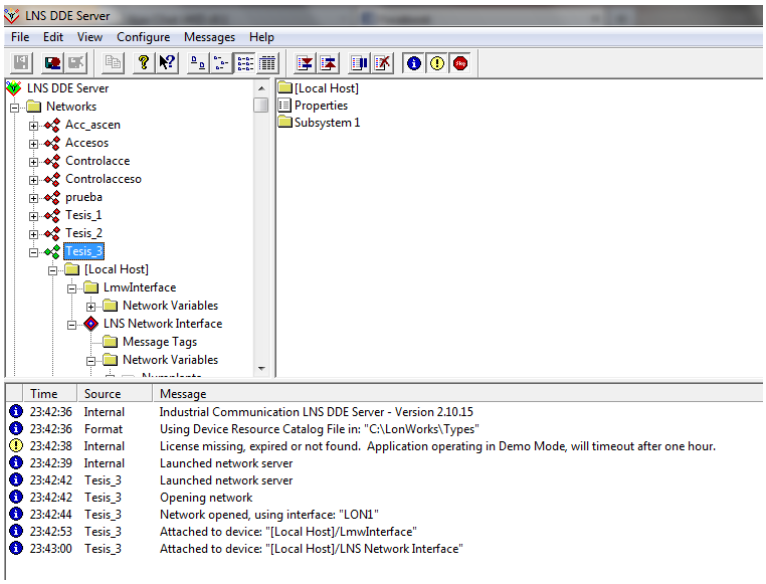


Figura. 1.41. LNS DDE Server

1.7.2. Comunicación PC – BASE DE DATOS

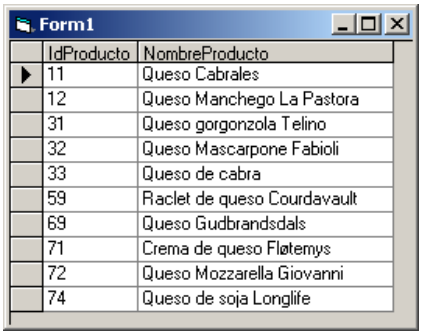


Figura. 1.42. Base de datos

En la actualidad existen muchos programas que permiten enlazarse con Visual Basic 6.0, tales como Oracle, SQLServer, Microsoft Access, etc.

Para el presente proyecto se decidió usar Microsoft Access, el cual se eligió ya que la creación de una base de datos con sus respectivas tablas se la puede

realizar gráficamente; que es una gran ayuda para el programador, además de que el manejo de los datos de las tablas en la base de datos es literalmente sencillo. Es importante mencionar que la interacción con Visual Basic es sencilla y robusta. La comunicación se realiza sin ningún inconveniente.

1.7.2.1. Creación de base de datos

Existen muchos motores para generar bases de datos como SQLServer Oracle, Microsoft Office Access. Se analizará en este caso Microsoft Office Access 2007; que es un motor fácil y amigable de usar; además que consta como en otros motores con una interfaz gráfica para su desarrollo.

1. Después de ingresar a Microsoft Office Access 2007, se selecciona Nuevo para crear una nueva base de datos.

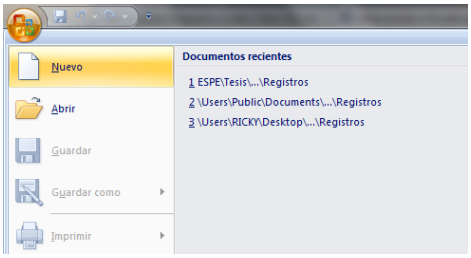


Figura. 1.43. Creación de base de datos

2. Inmediatamente, aparecerá la opción de la figura, en la que se escoge el nombre de la base de datos y el lugar donde se la va a guardar.

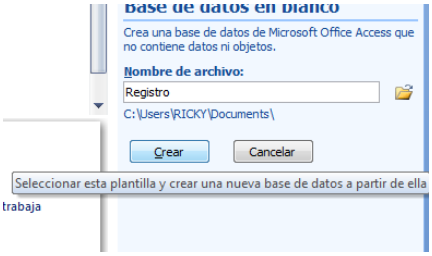


Figura. 1. 44. Asignación de nombre

3. A continuación, aparece la siguiente ventana en la que como muestra la figura se da click en **Tabla1**, y se accede a **Vista de diseño** en donde se puede configurar una tabla que se añade a la base de datos en creación.

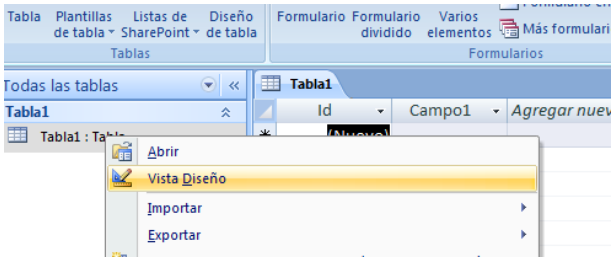


Figura. 1.45. Diseño de tabla

4. Primero de se debe asignar un nombre a la tabla, que en este caso es Accesos; como se ve en la figura.

En esta ventana permite ir ingresando cuales serán los campos o columnas de la tabla, y el tipo de dato que los registros o filas; que cada uno de los campos tendrán. Tal como en la figura, el tipo de dato para todos los campos es texto.

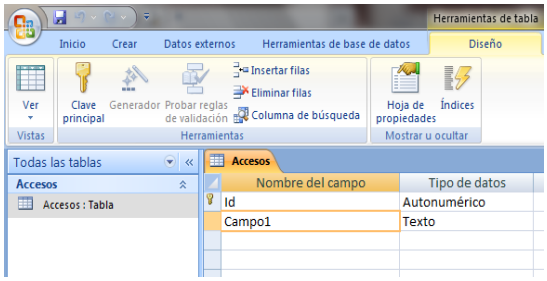


Figura. 1.46. Ingreso de campos

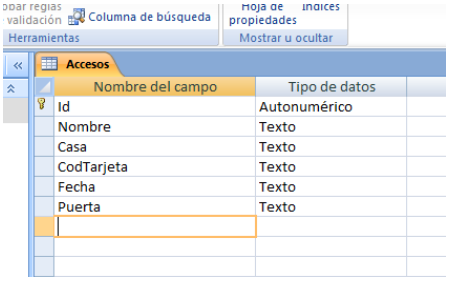


Figura. 1.47. Tipo de datos de campos

5. En la siguiente figura se muestra el diseño de la tabla, con sus respectivos campos, y los espacios para que sean llenados los registros de cada campo. Estos registros pueden ser añadidos desde esta misma ventana o desde una aplicación externa, como es el presente caso que se añaden datos desde el software de control de accesos.

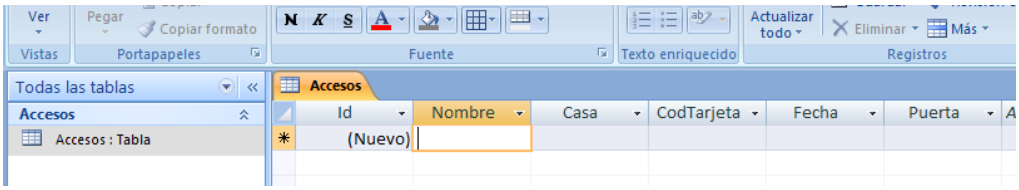


Figura. 1.48. Vista de tabla diseñada

Simplemente para poder crear más tablas para la misma base de datos se debe seguir el mismo procedimiento anterior.

6. Algo para aumentar la seguridad del sistema es importante contar con contraseña del archivo de la base de datos, pues mediante una instalación este archivo queda accesible para cualquier usuario: por lo que más que importante es necesario su uso.

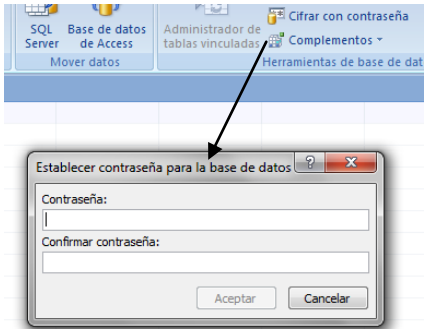


Figura. 1.49. Contraseña para base de datos

1.7.2.2. Mecanismo de comunicación con una base de datos

Existen algunos mecanismos para poder comunicarse con una determinada Base de Datos. Se analizará ADO.

ADO (ActiveX Data Objects)

ADO es una tecnología orientada a objetos para componentes ActiveX basada en una API en C++ llamada OLE DB.

ADO implementa drivers específicos para cada motor de base de datos en donde puede refinar el rendimiento para que estos trabajen perfectamente con cada tipo de base de datos.

ADO es una tecnología con la cual se puede leer, insertar, editar, borrar información de las tablas de una base de datos así como poder crear o eliminar tablas. Además es importante señalar que la programación de ADO es muy sencilla y amigable para el programador.

Algo importante para señalar es que OLE DB es quien coge los datos de una base de datos y ADO los presenta al programador. De esta forma, el programador no se preocupa de cómo se almacenan los datos, sólo de explotarlos.

- **Forma gráfica**

Para poder tener acceso a una base de datos desde Visual Basic 6.0 mediante el protocolo ADO pero en forma gráfica, deben utilizar los siguientes pasos:

1. Añadir el bloque de Adodc desde las herramientas de Visual Basic 6.0, a un formulario estándar donde queremos tener la conexión de una base de datos.

Figura. 1.50. Selección de modo base de datos

2. Para poder realizar la conexión con la base de datos se da click derecho en el bloque de Adodc en propiedades para proceder con la configuración.

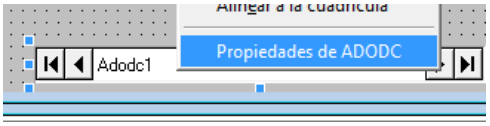


Figura. 1.51. Configuración de base de datos

3. En las siguientes figuras se ve el proceso a seguir para conseguir la conexión a la base de datos deseada, primero se selecciona **Generar** para escoger el proveedor de OLE DB, que será *"Microsoft Jet 4.0 OLE DB Provider"*, seleccionamos siguiente para examinar en la PC el lugar donde se encuentra la base de datos creada, para el caso se busca una base de datos .mdb, creada en Microsoft Access.

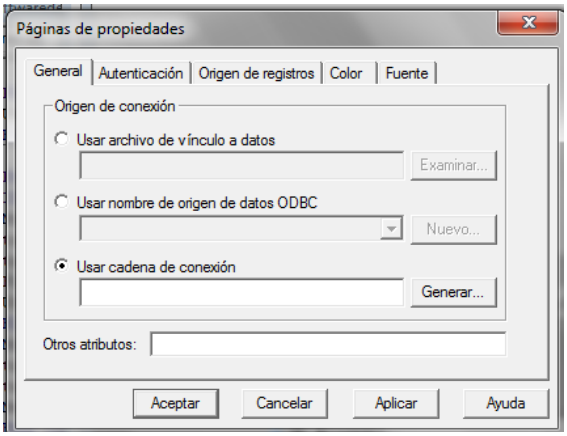


Figura. 1.52. Propiedades de base de datos

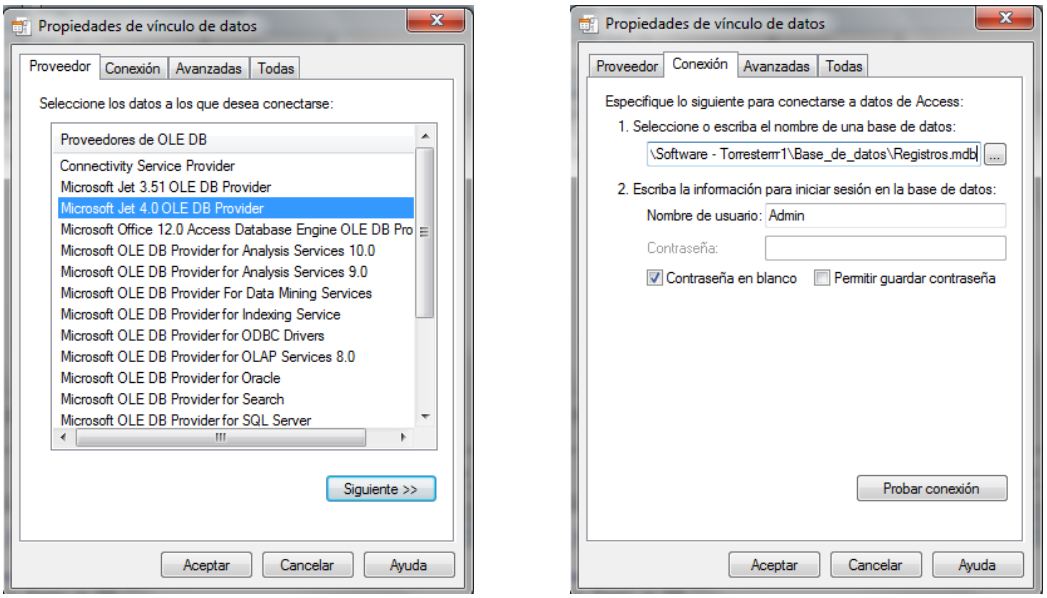


Figura. 1.53. Selección de proveedor de base de datos

4. Después se procede a ubicar la contraseña de la base de datos para poder tener acceso.

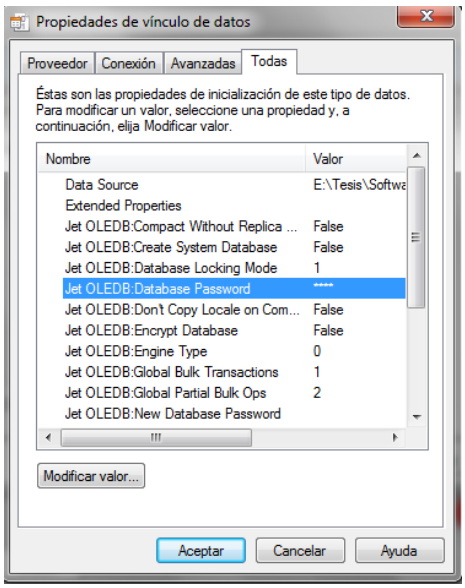


Figura. 1.54. Contraseña base de datos

5. Ahora para la conexión con una determinada tabla que contenga la base de datos es necesario mediante texto del comando SQL, seleccionar dicha tabla como se observa en la figura.

*Select * from (Tabla) Order by (Campo)*

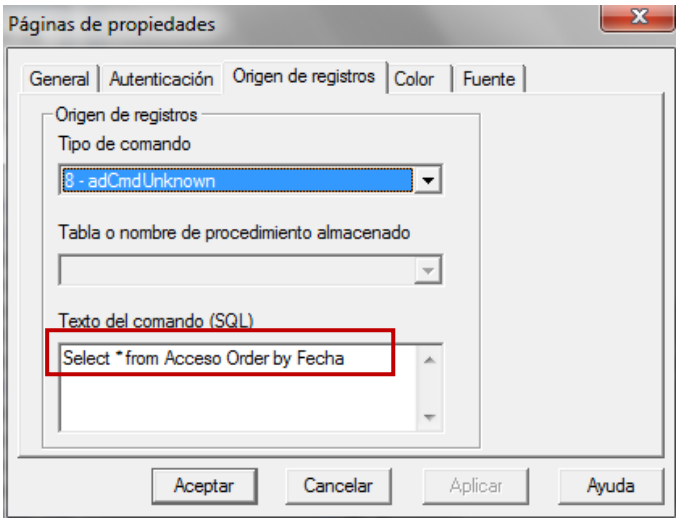


Figura. 1.55. Integrar base de datos

Para esta forma de conexión no es necesario crear un objeto para la acción *connection* y *recordset*, como tampoco abrir la base de datos y una tabla determinada con el comando *open* o cerrar las mismas con el comando *close;* puesto que la conexión a la base datos y una tabla ya se encuentran hechas, con el proceso indicado anteriormente.

Lo único que se debe realizar es la manipulación de los registros como mejor se requiera utilizar; ya sea para escribir, editar o eliminar. O bien sea el caso moverse a través de los registro de una determinada tabla.

Dicha manipulación se realiza mediante los mismos comandos que brinda Adodc dentro del Visual Basic 6.0, como por ejemplo:

- Me.Adodc1.Recordset.(1) → Selecciona el registro de la posición (1).
- Me.Adodc1.Recordset.AddNew → Añade datos a un registro.
- Me.Adodc1.Recordset.MoveNext → Sirve para moverse de un registro a otro.

CAPITULO II

SOFTWARE

2.1. INTRODUCCION

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.

2.1.1. 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.

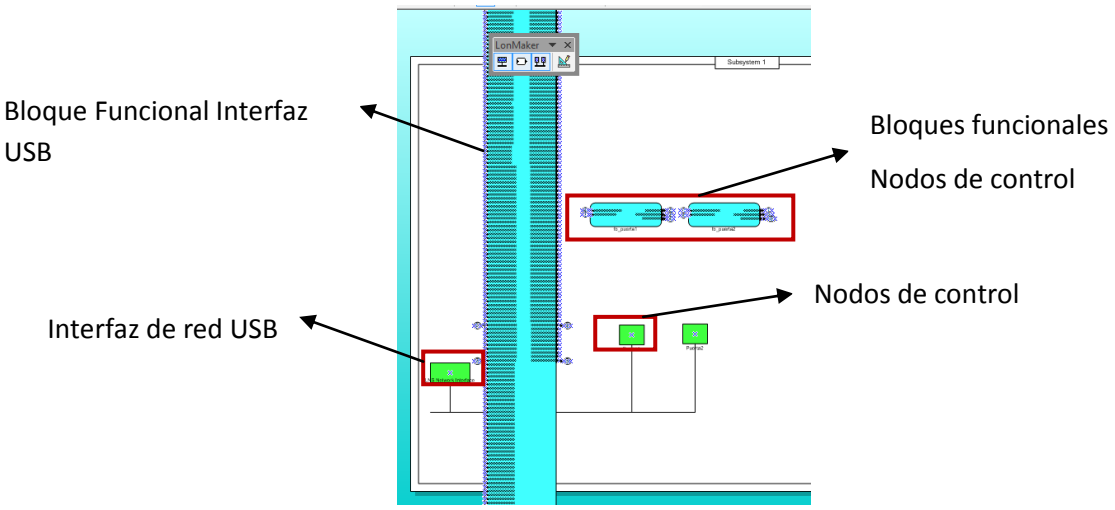


Figura. 2.1. Base de datos Lonmaker

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.

Teniendo presente este aspecto se podrá comprender de mejor manera la forma de comunicación PC - Nodo de control de accesos.

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 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 tacar 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

Para el presente trabajo se ve la necesidad de diseñar un software para un sistema de control de accesos, usando la tecnología Lonworks; que es implementada mediante los nodos de control de la marca ISDE.

Como se mencionó anteriormente el equipo a usar es el nodo de proximidad INP-120, 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.

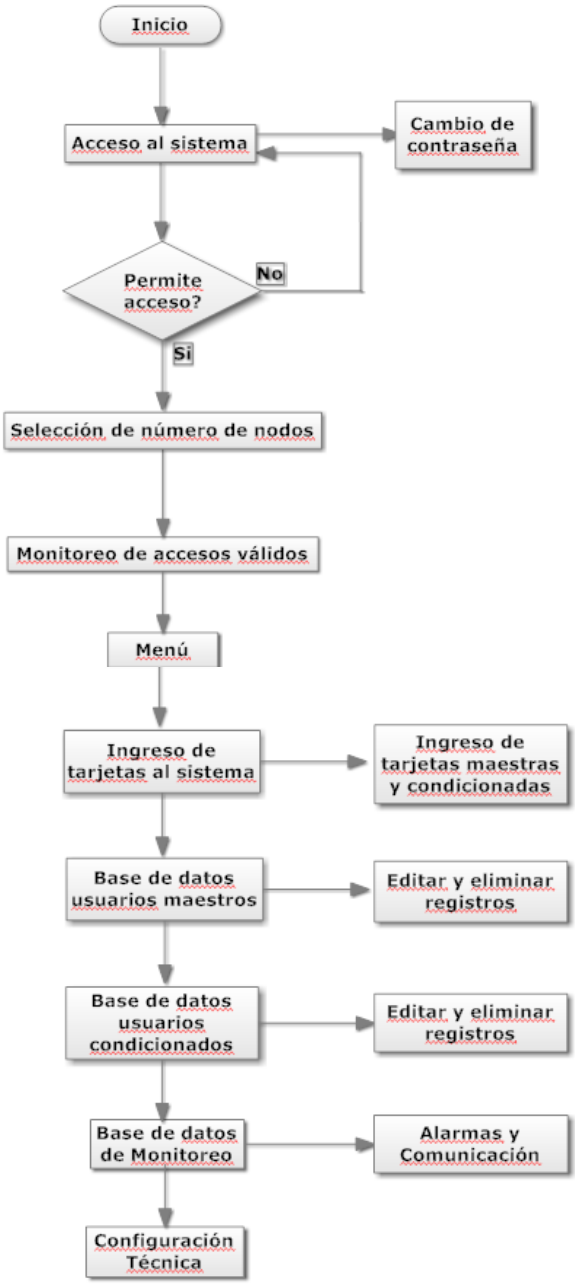


Figura. 2.2. Diagrama de flujo

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:

Para el diseño del software se tomarán en cuenta ciertos aspectos como son:

- Inicio del sistema
- Menú
- Ingreso de tarjetas:
    - Tarjetas maestras
    - Tarjetas condicionadas
- Base de datos:
    - Usuarios maestros
    - Usuarios condicionados
    - Monitoreo de accesos válidos
    - Alarmas
- 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, para las cuales se proporciona una porción de código para comprender mejor su funcionamiento:

2.3.1. Acceso Principal

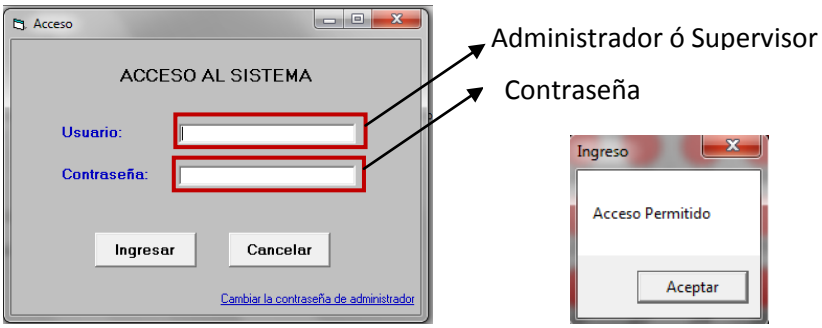


Figura. 2.3. Ventanas de acceso al sistema

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 (Figura. 2.4).

2.3.1.1. Tabla de datos contraseña

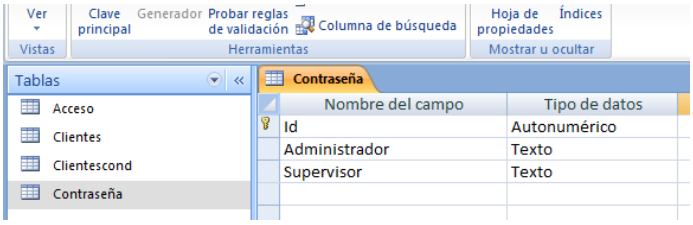


Figura. 2.4. Diseño de tabla Contraseña

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.

Es así que la comparación de contraseñas para el acceso al software es la siguiente:

- ***Código***

```
Me.Adodc1.Recordset.MoveFirst
'Recoge las claves de la base de datos'
a = Me.Adodc1.Recordset(1)
b = Me.Adodc1.Recordset(2)
'COMPARACION PARA ACCESO'
If (txtus.Text = "admin" And txtcontr.Text = a) Or (txtus.Text = "supervisor" And
txtcontr.Text = b) Then
MsgBox "Acceso Permitido", vbOKOnly, "Ingreso"
txtus.Enabled = False
txtcontr.Enabled = False
Form9.Show
Unload Me
recurso = Shell("C:\LonWorks\LNSDde\LNSDde.exe", vbHide)
Else
MsgBox "Acceso NO Permitido", vbOKOnly, "Ingreso"
txtus.Text = ""
txtcontr.Text = ""
Me.Show
End If
```

2.3.2. Cambio de Contraseña

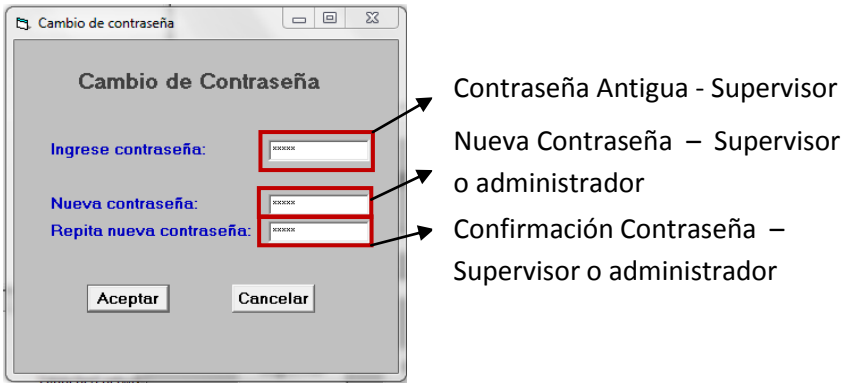


Figura. 2.5. Cambio de contraseña

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, como se lo explica en el Capítulo I 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.

*Select * from Contraseña*

- ***Código***

```
Dim a, b As String
Me.Adodc1.Recordset.Update
Me.Adodc1.Recordset.MoveFirst
a = Me.Adodc1.Recordset(1)
b = Me.Adodc1.Recordset(2)
If Anticont.Text = Me.Adodc1.Recordset(2) Then
   Select Case selección.Text
   Case "Administrador"
   If nuecont.Text = rencont.Text Then
```

Me.Adodc1.Recordset(1) = nuecont.Text

Sleep (500)

Me.Adodc1.Recordset.Update

MsgBox "La contraseña se cambio satisfactoriamente!!!", vbOKOnly, "Cambio de contraseña"

Acceso.Show

Unload Me

Else

MsgBox "La contraseña nueva deber ser la misma en ambos campos", vbOKOnly, "ERROR"

End If

Case "Supervisor"

If nuecont.Text = rencont.Text Then

Me.Adodc1.Recordset(2) = nuecont.Text

Sleep (500)

Me.Adodc1.Recordset.Update

MsgBox "La contraseña se cambio satisfactoriamente!!!", vbOKOnly, "Cambio de contraseña"

Acceso.Show

Unload Me

Else

MsgBox "La contraseña nueva deber ser la misma en ambos campos", vbOKOnly, "ERROR"

End If

End Select

Else

MsgBox "Contraseña no válida", vbOKOnly, "ERROR"

End If

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. 2.6 muestra, si se ingreso todos los datos correspondientes de la manera correcta.

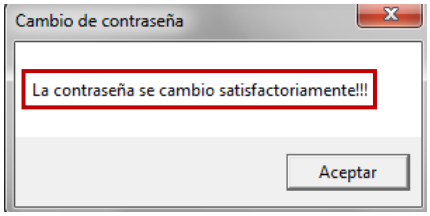


Figura. 2.6. Cambio de contraseña correcto

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

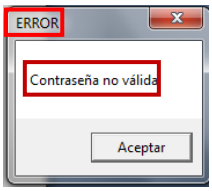


Figura. 2.7. Error contraseña

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

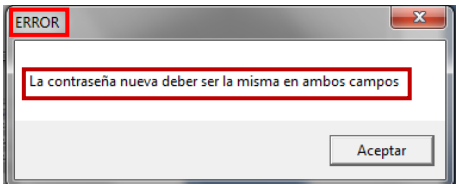


Figura. 2.8. Error nueva contraseña

2.3.3. Menú

Figura. 2.9. 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. 2.10. 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 solo es necesario conocer lo necesario de un usuario, así como: Nombre de la persona, identificación, departamento al que pertenece, acceso al cual se le quiere dar validez.

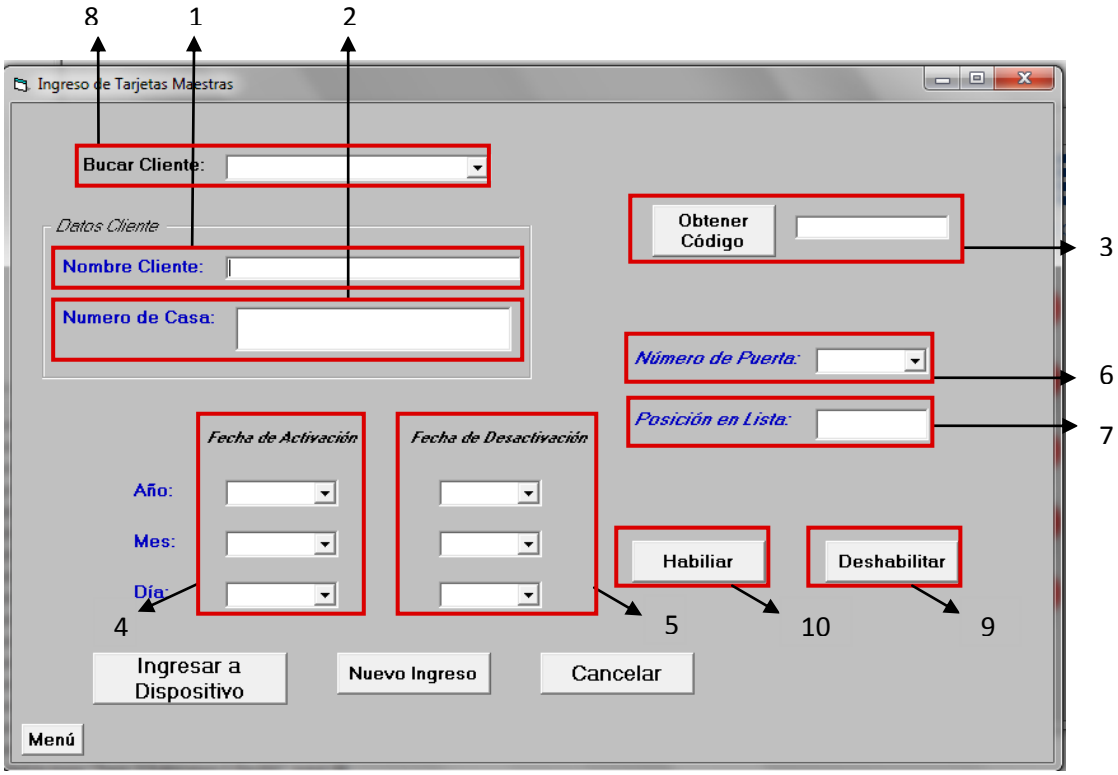


Figura. 2.11. Ingreso de Tarjetas Maestras

1. Nombre del cliente al cual se le designa una determinada tarjeta.
2. Número de casa al cual pertenece la persona a quien se le asigna una determinada tarjeta.
3. Se obtiene el código de la tarjeta que se quiere configurar (previamente se debe pasar la tarjeta a programar por el lector de proximidad).
4. Se configura el año, mes y día desde cuando la tarjeta podrá ser usada para un acceso válido.

5. Se configura el año, mes y día hasta cuando la tarjeta podrá ser usada para un acceso válido.
6. Se selecciona a que puerta se le quiere dar acceso con la tarjeta.
7. 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.
8. Esta opción le permite al administrador buscar dentro de la base de datos y recuperar los datos de un determinado usuario al cual se le quiere habilitar o deshabilitar el acceso al recinto.
9. Este botón le permite al administrador deshabilitar el acceso de una persona si así se lo requiere.
10. Este botón le permite al administrador habilitar el acceso a una persona, cuando previamente se lo ha deshabilitado.

a. 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**. Se ingresan los datos seleccionando **Ingresar a Dispositivo**.

- ***Código***

```
TarjetaMa.LinkMode = 0
TarjetaMa.LinkTopic = "LNSDDE|Tesis_3.Subsystem 1.DevNV"  'Servidor|Red'
'CONEXION CON EL NODO INP-120'
Call escri_datos
TarjetaMa.LinkTimeout = 100
TarjetaMa.LinkMode = 1
'INGRESA DATOS DE TARJETA AL NODO INP-120'
TarjetaMa.Text = "0" + "," + poslist.Text + "," + "1" + "," + codigo.Text + "," + c(1) + "," + m + "," + Diaini.Text + "," + d(1) + "," + n + "," + Diafin.Text + "," + "0" + "," + p + "," + tipusu.Text + "," + nivusu.Text + "," + "0"
TarjetaMa.LinkPoke
```

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.

- ***Código***

```
'CONEXION DE BASE DE DATOS'
'ASIGNA LOS VALORES A LA BASE DE DATOS'
Me.Adodc1.Recordset.AddNew
    Me.Adodc1.Recordset(1) = Nombre.Text
    Me.Adodc1.Recordset(2) = Vivienda.Text
    Me.Adodc1.Recordset(3) = codigo.Text
    Me.Adodc1.Recordset(4) = a + "/" + m + "/" + Diaini.Text
    Me.Adodc1.Recordset(5) = b + "/" + n + "/" + Diafin.Text
    Me.Adodc1.Recordset(6) = numpuerta2.Text
    Me.Adodc1.Recordset(7) = poslist.Text
    Me.Adodc1.Recordset(8) = tipusu.Text
    Me.Adodc1.Recordset(9) = nivusu.Text
Me.Adodc1.Recordset.Update
```

b. Dentro de esta ventana tenemos la posibilidad de dar de baja a una tarjeta de acceso momentáneamente y a esta misma dar de alta; mediante la pestaña **Buscar Cliente,** que muestra los usuarios dentro de la base de datos correspondiente.

En la ventana de ingreso de tarjetas maestras, en vez de ingresar los datos en cada uno de los campos; se selecciona del buscador a que usuario se le quiere habilitar o deshabilitar. Al momento de seleccionar un usuario se cargan lo 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.

- **Deshabilitar**

Primero se debe consultar a los usuarios de la base de datos que tienen accesos al recinto.

- ***Código***

'PERMITE BUSCAR UN USUARIO DE LA BASE DE DATOS DE USUARIOS MAESTROS Y UBICARLOS EN LA VENTANA DE INGRESO DE TARJETAS MAESTRAS'

```
separador = ","
separador2 = "/"
q = comnombre.Text
n = Me.Adodc1.Recordset.RecordCount
If n > 0 Then
Me.Adodc1.Recordset.MoveFirst
p = Me.Adodc1.Recordset(1)
For e = 1 To n
p = Me.Adodc1.Recordset(1)
If p = q Then
Nombre.Text = Me.Adodc1.Recordset(1)
Vivienda.Text = Me.Adodc1.Recordset(2)
codigo.Text = Me.Adodc1.Recordset(3)
auxfealta.Text = Me.Adodc1.Recordset(4)
auxfebaja.Text = Me.Adodc1.Recordset(5)
partes2 = Split(auxfealta, separador2)
    Añoini.Text = partes2(0)
    Mesini.Text = partes2(1)
    Diaini.Text = partes2(2)
partes3 = Split(auxfebaja, separador2)
    Añofin.Text = partes3(0)
    Mesfin.Text = partes3(1)
    Diafin.Text = partes3(2)
```

numpuerta2.Text = Me.Adodc1.Recordset(6)
poslist.Text = Me.Adodc1.Recordset(7)
tipusu.Text = Me.Adodc1.Recordset(8)
nivusu.Text = Me.Adodc1.Recordset(9)
End If
Me.Adodc1.Recordset.MoveNext
Next
End If

Después de consultados los registros de la base de datos, se procede a deshabilitar la tarjeta, para ello solo se ingresa una fecha de desactivación que ya ha pasado y así poder impedir el acceso al recinto a un determinado usuario, pero dicha información no se ingresa en le base de datos pues esto se lo usa para deshabilitar a un usuario momentáneamente.

- ***Código***

'DESHABILITA UNA TARJETA'
TarjetaMa.LinkMode = 0
TarjetaMa.LinkTopic = "LNSDDE|Tesis_3.Subsystem 1.DevNV" 'Servidor|Red'
Call escri_datos
TarjetaMa.LinkTimeout = 100
TarjetaMa.LinkMode = 1
'INGRESA DATOS DE TARJETA AL NODO INP-120'
TarjetaMa.Text = "0" + "," + poslist.Text + "," + "1" + "," + codigo.Text + "," + "10" + "," + "1" + "," + "1" + "," + "10" + "," + "2" + "," + "1" + "," + "0" + "," + p + "," + tipusu.Text + "," + nivusu.Text + "," + "0"
TarjetaMa.LinkPoke

- **Habilitar**

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 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. Para el ingreso de este tipo de tarjetas es necesario conocer lo necesario de un usuario, así como: Nombre de la persona, identificación, departamento al que pertenece, acceso al cual se le quiere dar validez. Generalmente este tipo de tarjetas se les asigna a personas de la limpieza o mantenimiento que deben ingresar solo ciertos días y horas determinadas.

El ingreso de este tipo de tarjetas es similar para el ingreso de tarjetas maestras, a diferencia que se ataca a la variable **nviConfHoraria**, y sus datos son registrados en la tabla Clientescond de la base de datos; mediante la conexión que se realizará con un objeto ADODC. Se ingresan los datos tras seleccionar todos los campos necesarios.

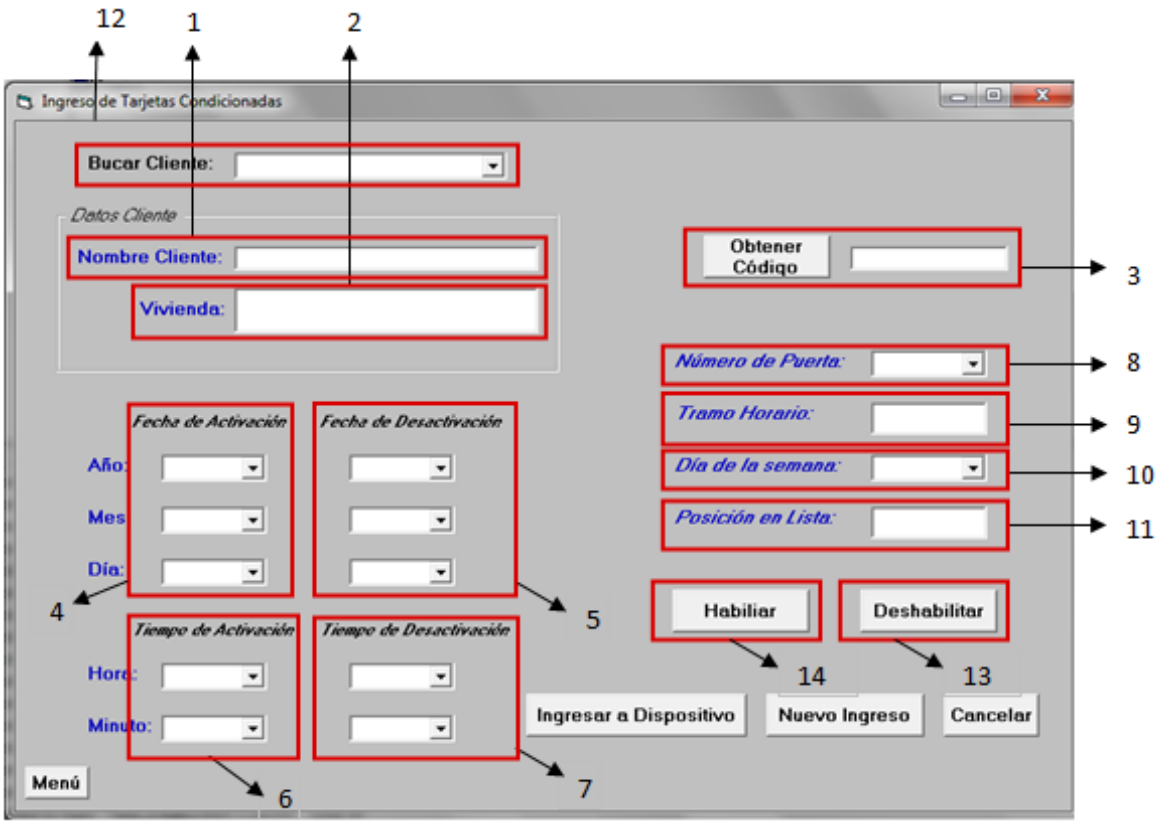


Figura. 2.12. Ingreso de Tarjetas Condicionadas

1. Nombre del cliente al cual se le designa una determinada tarjeta.
2. Número de casa al cual pertenece la persona a quien se le asigna una determinada tarjeta.
3. Se obtiene el código de la tarjeta que se quiere configurar (previamente se debe pasar la tarjeta a programar por el lector de proximidad).
4. Se configura el año, mes y día desde cuando la tarjeta podrá ser usada para un acceso válido.
5. Se configura el año, mes y día hasta cuando la tarjeta podrá ser usada para un acceso válido.
6. Se configura la hora y minuto desde cuando la tarjeta podrá ser usada para un acceso válido.
7. Se configura la hora y minuto hasta cuando la tarjeta podrá ser usada para un acceso válido.
8. Se selecciona a que puerta se le quiere dar acceso con la tarjeta.

9. Indica el tramo horario del día se quiere configurar, el equipo tiene hasta dos tramos horarios
10. Se escoge el día de la semana en el cual se aplicará el horario elegido en los pasos 4, 5, 6 y 7.
11. 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.
12. Esta opción le permite al administrador buscar dentro de la base de datos y recuperar los datos de un determinado usuario al cual se le quiere habilitar o deshabilitar el acceso al recinto.
13. Este botón le permite al administrador deshabilitar el acceso de una persona si así se lo requiere.
14. Este botón le permite al administrador habilitar el acceso a una persona, cuando previamente se lo ha deshabilitado.

a. 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**.

- **Deshabilitar**

Para este caso, la ventana también consta de un buscador de los usuarios registrados en la base de datos correspondiente; de la misma manera se consultan los datos del usuario a deshabilitar. Tal como en los usuarios maestros se ingresa una fecha que ya ha pasado para la des habilitación momentánea.

- **Habilitar**

Para la habilitación de un usuario, de la misma manera se busca el usuario al que se le quiere habilitar recuperando los registros de la base de datos e ingresándolos de nuevo al sistema. Al igual que los usuarios maestros, también

debe haber sido previamente deshabilitada una tarjeta para que tenga un uso la función de habilitar.

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 siguientes campos:

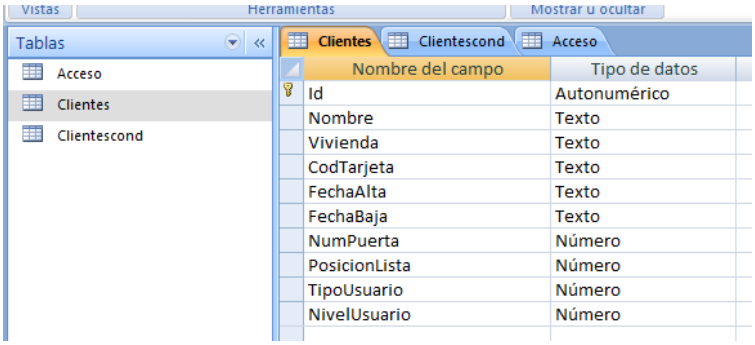


Figura. 2.13. Diseño de tabla Clientes

En la figura. 2.9, se puede ver cada uno de los campos de los usuarios que se guardarán en la base de datos, y el tipo de dato que esta contendrá.

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 añadir un objeto del tipo datagrid para poder conectar con la tabla 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.

1. Para consultar los datos de la tabla Clientes con comandos SQL.

*Select * from Clientes*

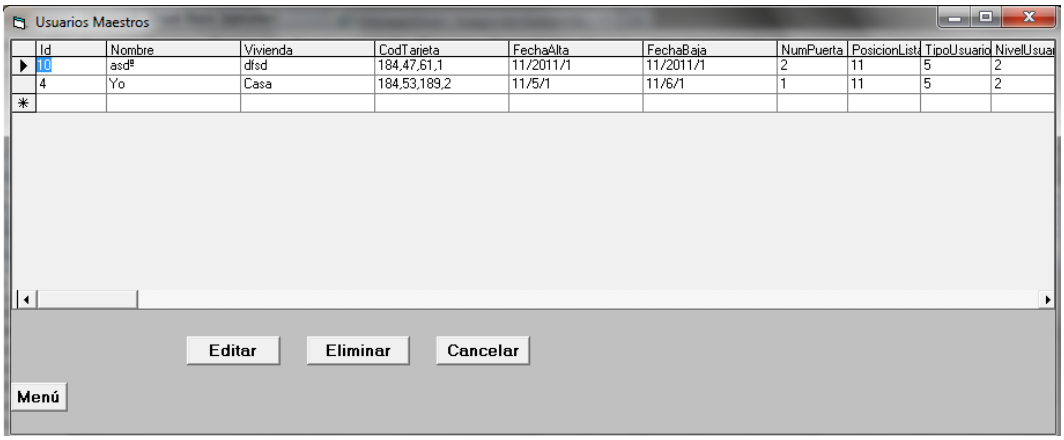


Figura. 2.14. Ventana tabla de datos de usuarios maestros

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.

- **Eliminar**

Para eliminar a un usuario seleccionando de la tabla primero de detecta que la tabla tenga algún registro:

- ***Código***

```
If grdDataGrid.Row = -1 Then
    MsgBox "No hay ningún registro para eliminar", vbInformation
    Exit Sub
End If
With grdDataGrid
    If MsgBox("Se va a eliminar el registro : está seguro ", _
            vbExclamation + vbYesNo, "Beliminar_Click") = vbYes Then
```

Si existe algún registro dentro de la tabla se procede a borrar la información seleccionada.

Primero se consultan los datos de la tabla de datos del registro seleccionado para poder extraer los datos necesarios en insertar en el nodo para poder borrar la información.

- ***Código***

```
bNombre.Text = Me.Adodc1.Recordset("Nombre")
bNombre.Text = Me.Adodc1.Recordset(1)
Vivienda.Text = Me.Adodc1.Recordset(2)
separador = ","
auxcod.Text = Me.Adodc1.Recordset(3)
partes = Split(auxcod, separador)
    cod1.Text = partes(0)
    cod2.Text = partes(1)
    cod3.Text = partes(2)
    cod4.Text = partes(3)
numpuerta.Text = Me.Adodc1.Recordset(6)
poslist.Text = Me.Adodc1.Recordset(7)
'BORRAR DATOS EN EL NODO INP-120'
TarjetaMabo.LinkMode = 0
TarjetaMabo.LinkTopic = "LNSDDE|Tesis_3.Subsystem 1.DevNV"
Call escri_datos
TarjetaMabo.LinkTimeout = 100
TarjetaMabo.LinkMode = 1
TarjetaMabo.Text = ""
TarjetaMabo.Text = "0" + "," + poslist.Text + "," + "3" + "," + cod1.Text + "," +
cod2.Text + "," + cod3.Text + "," + cod4.Text + "," + "0" + "," + "0" + "," + "0" + "," +
"0" + "," + "0" + "," + "0" + "," + "0" + "," + numpuerta.Text + "," + "5" + "," + "2" + ","
+ "0"
TarjetaMabo.LinkPoke
```

Después de realizado este paso se borra de la base de datos

Me.Adodc1.Recordset.Delete

- **Editar**

Para editar se debe escoger primero un registro. Se consultan los datos de este registro, y se agrega estos a textos auxiliares que permiten enviar los datos del registro al nodo para eliminar la configuración establecida.

- ***Código***

```
bNombre.Text = Me.Adodc1.Recordset("Nombre")
bNombre.Text = Me.Adodc1.Recordset(1)
Vivienda.Text = Me.Adodc1.Recordset(2)
auxcod.Text = Me.Adodc1.Recordset(3)
partes4 = Split(auxcod, separador)
    cod1.Text = partes4(0)
    cod2.Text = partes4(1)
    cod3.Text = partes4(2)
    cod4.Text = partes4(3)
numpuerta.Text = Me.Adodc1.Recordset(6)
poslist.Text = Me.Adodc1.Recordset(7)
'BORRAR DATOS EN EL NODO INP-120'
TarjetaMabo.LinkMode = 0
TarjetaMabo.LinkTopic = "LNSDDE|Tesis_3.Subsystem 1.DevNV"
Call escri_datos
TarjetaMabo.LinkTimeout = 100
TarjetaMabo.LinkMode = 1
TarjetaMabo.Text = ""
TarjetaMabo.Text = "0" + "," + poslist.Text + "," + "3" + "," + cod1.Text + "," +
cod2.Text + "," + cod3.Text + "," + cod4.Text + "," + "0" + "," + "0" + "," + "0" + "," +
```

"0" + "," + "0" + "," + "0" + "," + "0" + "," + numpuerta.Text + "," + "5" + "," + "2" + "," + "0"
TarjetaMabo.LinkPoke

Dichos datos también se usan para los campos correspondientes en la ventana de ingreso de tarjetas maestras; desde donde se podrá cambiar cualquier dato que se requiera cambiar

- ***Código***

```
Tarjetas_Maestras.Nombre.Text = Me.Adodc1.Recordset("Nombre")
Tarjetas_Maestras.Nombre.Text = Me.Adodc1.Recordset(1)
Tarjetas_Maestras.Vivienda.Text = Me.Adodc1.Recordset(2)
Tarjetas_Maestras.codigo.Text = Me.Adodc1.Recordset(3)
Tarjetas_Maestras.auxfealta.Text = Me.Adodc1.Recordset(4)
Tarjetas_Maestras.auxfebaja.Text = Me.Adodc1.Recordset(5)
partes2 = Split(Tarjetas_Maestras.auxfealta, separador2)
    Tarjetas_Maestras.Añoini.Text = partes2(0)
    Select Case partes2(1)
    Case 1
    Tarjetas_Maestras.Mesini.Text = "Enero"
    Case 2
    Tarjetas_Maestras.Mesini.Text = "Febrero"
    Case 3
    Tarjetas_Maestras.Mesini.Text = "Marzo"
    Case 4
    ...
    ...
    End Select
    Tarjetas_Maestras.Diaini.Text = partes2(2)
partes3 = Split(Tarjetas_Maestras.auxfebaja, separador2)   'Separa cadena de caracteres (split)'
```

Tarjetas_Maestras.Añofin.Text = partes3(0)

Select Case partes3(1)

Case 1

Tarjetas_Maestras.Mesfin.Text = "Enero"

Case 2

Tarjetas_Maestras.Mesfin.Text = "Febrero"

Case 3

Tarjetas_Maestras.Mesfin.Text = "Marzo"

Case 4

...

...

End Select

Tarjetas_Maestras.Diafin.Text = partes3(2)

Tarjetas_Maestras.numpuerta.Text = Me.Adodc1.Recordset(6)

...

...

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 siguiente la tabla llamada Clientescond que tendrá los siguientes campos:

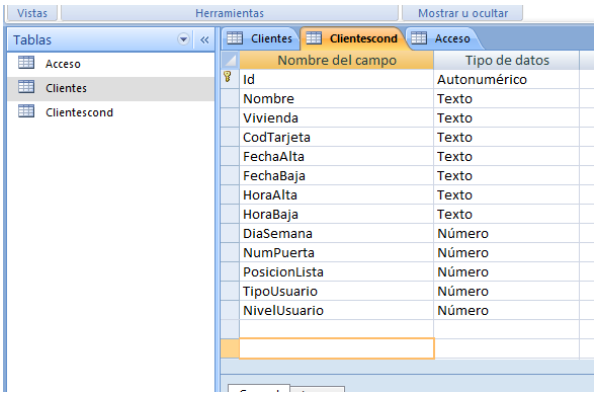


Figura. 2.15. Diseño de tabla Clientescond

En la Figura. 2.15 se puede ver cada uno de los campos de los usuarios que se guardarán en la base de datos, y el tipo de dato que esta contendrá.

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.

Además de que mediante el comando SQL, se llama a esta tabla:

*Select * from (Clientescond) Order by Fecha*

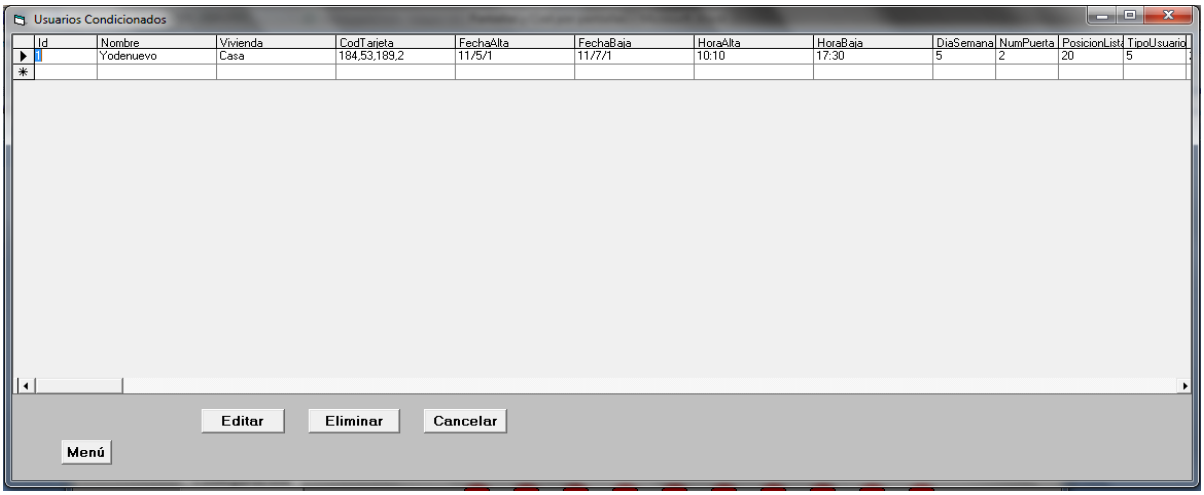


Figura. 2.16. Ventana de tabla de datos de usuarios condicionados

Al igual que en la base anterior, se tiene la opción de eliminar y editar; que para el caso es el mismo procedimiento recordando que:

- **Eliminar**

Para eliminar se debe recordar que en esta nueva tabla se tienen más campos y para ellos existen nuevos datos que deben ser consultados para la acción requerida.

- **Editar**

Para editar se debe recordar que los campos a donde serán enviados los datos consultados de este tabla será a la ventana de ingreso de tarjetas condicionadas; desde donde se podrá realizar los cambios deseados.

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.

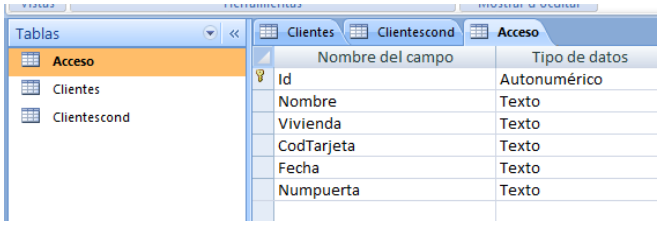


Figura. 2.17. Diseño de tabla Acceso

Se consultan los registros de la tabla también con comandos SQL

*Select * from (Accesos) Order by Fecha*

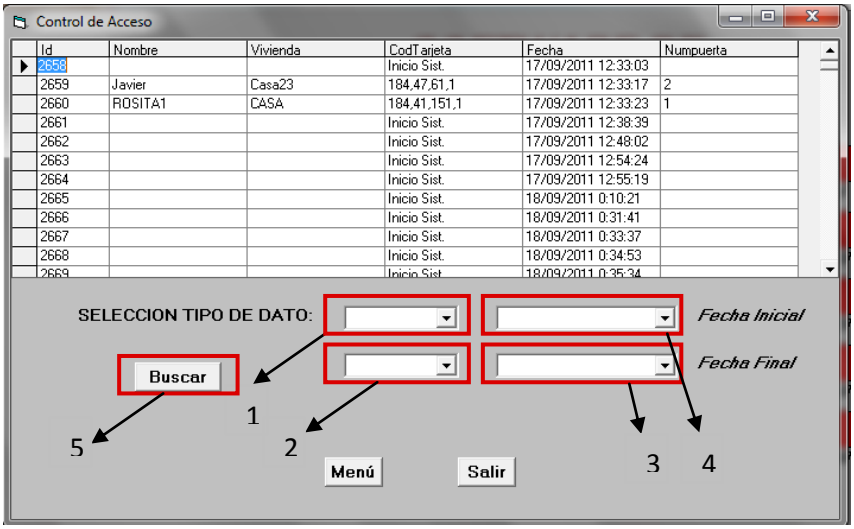


Figura. 2.18. Ventana de tabla de datos de control de acceso

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.

A continuación, se muestra el código necesario para poder filtrar los datos deseados (el código tanto para filtrar por nombre o por vivienda son similares, más información en los anexos):

- **Código**

```
Dim b, c, k, j, i, m, n, o, p As Integer
c = Filtro.Adodc1.Recordset.RecordCount
For i = 1 To c
Filtro.Adodc1.Recordset.Delete
Filtro.Adodc1.Recordset.MoveNext
Next
b = Me.Adodc1.Recordset.RecordCount
Select Case selec.Text
Case "Nombre"                    'Filtrar por nombre'
Me.Adodc1.Recordset.MoveFirst
For j = 1 To b
If Me.Adodc1.Recordset(1) = tipo.Text Then
Filtro.Adodc1.Recordset.AddNew          'Asignación de datos en nueva tabla'
Filtro.Adodc1.Recordset(1) = Me.Adodc1.Recordset(1)
Filtro.Adodc1.Recordset(2) = Me.Adodc1.Recordset(2)
Filtro.Adodc1.Recordset(3) = Me.Adodc1.Recordset(3)
Filtro.Adodc1.Recordset(4) = Me.Adodc1.Recordset(4)
Filtro.Adodc1.Recordset(5) = Me.Adodc1.Recordset(5)
End If
Me.Adodc1.Recordset.MoveNext
Next
Me.Adodc1.Recordset.MoveFirst
Case "Fecha"                     'Filtrar por fecha'
Me.Adodc1.Recordset.MoveFirst
For j = 1 To b
If Me.Adodc1.Recordset(4) = fechaini.Text Then
n = Me.Adodc1.Recordset.AbsolutePosition
```

```
End If
If Me.Adodc1.Recordset(4) = fechafin.Text Then
o = Me.Adodc1.Recordset.AbsolutePosition
End If
Me.Adodc1.Recordset.MoveNext
Next
Me.Adodc1.Recordset.MoveFirst
'Sleep (500)
For m = 1 To b
If Me.Adodc1.Recordset(4) = fechaini.Text Then
For p = n To o
Filtro.Adodc1.Recordset.AddNew          'Asignación de datos en nueva tabla'
Filtro.Adodc1.Recordset(1) = Me.Adodc1.Recordset(1)
Filtro.Adodc1.Recordset(2) = Me.Adodc1.Recordset(2)
Filtro.Adodc1.Recordset(3) = Me.Adodc1.Recordset(3)
Filtro.Adodc1.Recordset(4) = Me.Adodc1.Recordset(4)
Filtro.Adodc1.Recordset(5) = Me.Adodc1.Recordset(5)
Me.Adodc1.Recordset.MoveNext
Next
m = o + 2
End If
Me.Adodc1.Recordset.MoveNext
Next
Me.Adodc1.Recordset.MoveFirst
End Select
Filtro.Show
End Sub
```

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.

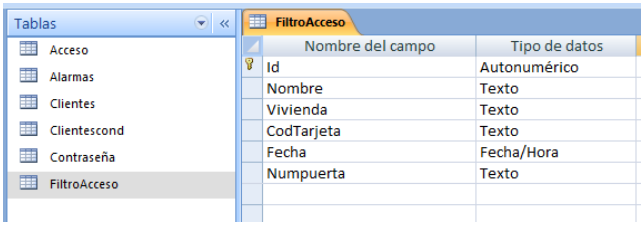
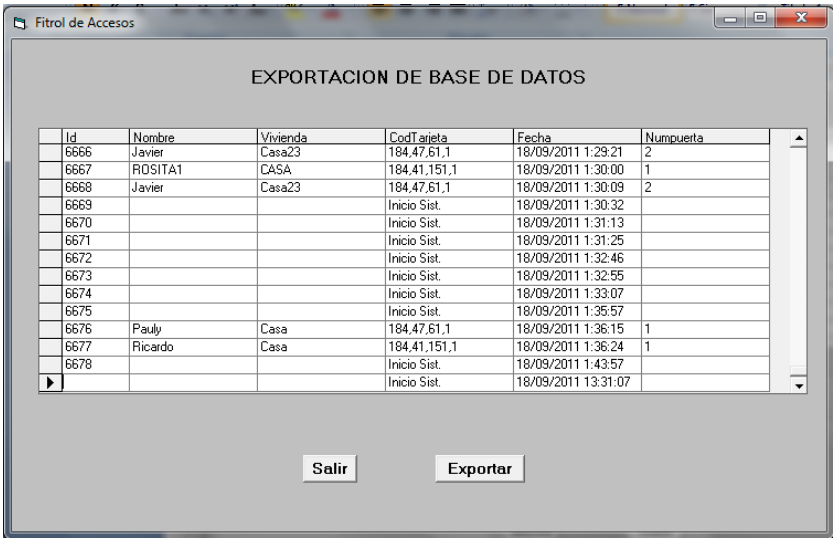


Figura. 2.19. Diseño de tabla FiltroAcceso

Se consultan los registros de la tabla también con comandos SQL

*Select * from (FiltroAcceso) Order by Fecha*



Id	Nombre	Vivienda	CodTarjeta	Fecha	Numpuerta
6666	Javier	Casa23	184,47,61,1	18/09/2011 1:29:21	2
6667	ROSITA1	CASA	184,41,151,1	18/09/2011 1:30:00	1
6668	Javier	Casa23	184,47,61,1	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	Pauly	Casa	184,47,61,1	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	
			Inicio Sist.	18/09/2011 13:31:07	

Figura. 2.20. 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**

- **Código**

‘Condiciona si existen valores en los registros de la tabla’

If Filtro.Adodc1.Recordset.RecordCount <> 0 Then

'Crear un objeto del tipo excel.application

Set objExcel = New Excel.Application

objExcel.Visible = True

objExcel.SheetsInNewWorkbook = 1

objExcel.Workbooks.Add

'PONER UN TITULO

objExcel.ActiveSheet.Cells(2, 4) = "BASE DE DATOS DEL CONTROL DE ACCESOS DEL RECINTO"

'UTILIZAMOS LAS VARIABLES PARA LA UBICACION DE NUESTROS TEXTOS’

HNom = 1

VNom = 5

Vdatos = 6

Hdatos = 1

cuentaNombres = Filtro.Adodc1.Recordset.Fields.Count

cuentadatos = Filtro.Adodc1.Recordset.RecordCount

'AGREGAMOS LOS REGISTROS (RECUERDEN QUE NO IMPORTA CUANTAS COLUMNAS O REGISTROS TENGAMOS EL BUCLE_

'FUNCIONA SEGUN EL NUMERO DE CABECERAS Y REGISTROS

objExcel.Columns("E").Select

objExcel.Selection.NumberFormat = "dd/MM/yyyy hh:mm:ss" **‘Formato para la celda de fecha’**

For i = 0 To (cuentaNombres - 1) **‘Exportación de campos de la tabla a la hoja de excel**

objExcel.ActiveSheet.Cells(VNom, HNom) =

Filtro.Adodc1.Recordset.Fields(i).Name 'rstFacturas.Fields(i).Name

HNom = HNom + 1

Next

n = 0

```
Filtro.Adodc1.Recordset.MoveFirst
For n = 1 To cuentadatos          'Exportación de registros de la tabla a la hoja de excel'
objExcel.ActiveSheet.Cells(Vdatos, Hdatos + 0) = Filtro.Adodc1.Recordset(0)
objExcel.ActiveSheet.Cells(Vdatos, Hdatos + 1) = Filtro.Adodc1.Recordset(1)
objExcel.ActiveSheet.Cells(Vdatos, Hdatos + 2) = Filtro.Adodc1.Recordset(2)
objExcel.ActiveSheet.Cells(Vdatos, Hdatos + 3) = Filtro.Adodc1.Recordset(3)
objExcel.ActiveSheet.Cells(Vdatos, Hdatos + 4) = Filtro.Adodc1.Recordset(4)
objExcel.ActiveSheet.Cells(Vdatos, Hdatos + 5) = Filtro.Adodc1.Recordset(5)
Vdatos = Vdatos + 1
Filtro.Adodc1.Recordset.MoveNext
Next
Hdatos = Hdatos + 1
Vdatos = 6
Filtro.Adodc1.Recordset.MoveFirst
End If
Exit Sub
ErrorExcel:
MsgBox Err.Description
```

2.3.5.5. Base de datos de alarmas

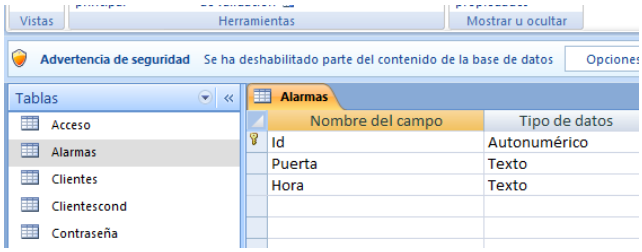


Figura. 2.21. Diseño de tabla Alarmas

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.

Se deben recoger los datos de la base de datos, mediante el objeto ADODC, que toma el nombra de adodc1, el objeto datagrid que como fuente de datos escoge a adodc1 y mediante los comandos SQL

*Select * from Alarmas Order by Fecha*

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. 2.22. Ventana de aviso de alarmas

2.3.6. Monitoreo

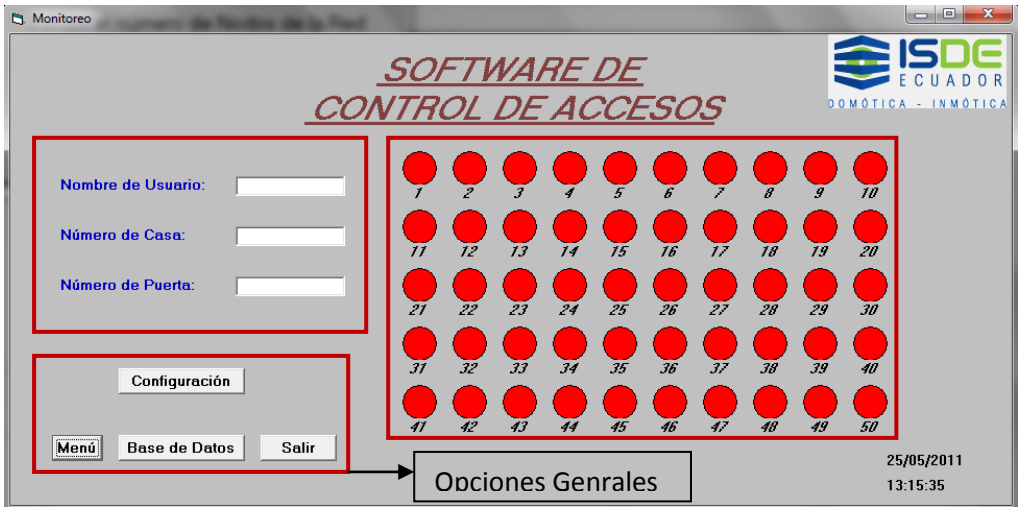


Figura. 2.23. Monitoreo del sistema

a. 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 del 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.**

- ***Código***

'EJEMPLO DE UN SOLO ACCESO'

```
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
```

b. 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.

- ***Código***

‘LECTURA SOLO DE UN LECTOR DE PROXIMIDAD’

```
Function lecturas() As String
Dim pa() As String
Dim separador4 As String
separador4 = ","
Text10(0).LinkMode = 0
Text10(0).LinkTopic = "LNSDDE|Tesis_3.Subsystem 1.DevNV"
Text10(0).LinkItem = "LNS Network Interface.nvoDatosLeidosVr -t RAW"
Text10(0).LinkTimeout = 100
Text10(0).LinkMode = 1
pa = Split(Text10(0), separador4) 'Separa el String que se capta del Nodo'
lecturas = pa(2) + "," + pa(3) + "," + pa(4) + "," + pa(5)
End Function
```

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.

Para poder extraer de esta variable solo los datos deseados, se hace lo siguiente:

- ***Código***

```
separador4 = ","
pa = Split(Text10(0), separador4) 'Separa el String que se capta del Nodo'
lecturas = pa(2) + "," + pa(3) + "," + pa(4) + "," + pa(5)
```

c. 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.

Así se podrá consultar las bases de datos de los usuarios maestros, condicionados y poder añadir información a la base de datos para el monitoreo.

- ***Código***

```
'NODO 1'
'ACTIVA INDICADOR SI EXISTE UN ACCESO VÁLIDO'
If a(0) = 1 Then
Nombre.Text = ""
Vivienda.Text = ""
numpuerta.Text = ""
estpuerta(0).FillColor = RGB(0, 255, 0)
separador4 = ","
ban.Text = "1"
End If
'ACTIVA INDICADOR SI EXISTE UN ACCESO NO VÁLIDO'
If (a(0) = 0 And ban.Text = "1") Then
estpuerta(0).FillColor = RGB(255, 0, 0)
'BUSCA EN BASE DE DATOS DE USUARIOS MAESTROS'
```

cod.Text = lecturas **‘Extrae el código leído en la función lecturas’**

numpuerta.Text = ”TorreA” **'Indica la puerta de acceso válido'**

Call basema

'BUSCA EN BASE DE DATOS DE USUSARIOS CONDICIONADOS'

Call basecond

'Se escoge solo los caracteres que indican el codigo de tarjeta'

Call basecontr

ban.Text = "0"

End If

Esta estructura se debe repetir para cada uno de los nodos conectados en el sistema. A continuación se muestra el acceso a las tablas de la base de datos.

- ***Código***

Private Sub basema()

'BUSCA EN BASE DE DATOS DE USUARIOS MAESTROS'

Dim c As String

Dim b, i As Integer

b = Me.Adodc1.Recordset.RecordCount

If b > 0 Then

Me.Adodc1.Recordset.MoveFirst

c = Me.Adodc1.Recordset(3)

For i = 1 To b

c = Me.Adodc1.Recordset(3)

If c = cod.Text Then

i = b + 1

Nombre.Text = Me.Adodc1.Recordset(1)

Vivienda.Text = Me.Adodc1.Recordset(2)

End If

Me.Adodc1.Recordset.MoveNext

Next

End If

```
End Sub
Private Sub basecond()
'BUSCA EN BASE DE DATOS DE USUSARIOS CONDICIONADOS'
Dim c As String
Dim d, i As Integer
d = Me.Adodc2.Recordset.RecordCount
If d > 0 Then
Me.Adodc2.Recordset.MoveFirst
c = Me.Adodc2.Recordset(3)
For i = 1 To d
c = Me.Adodc2.Recordset(3)
If c = cod.Text Then
i = b + 1
Nombre.Text = Me.Adodc2.Recordset(1)
Vivienda.Text = Me.Adodc2.Recordset(2)
End If
Me.Adodc2.Recordset.MoveNext
Next
End If
End Sub
Private Sub basecontr()
'SE ESCOGE CARACTERES QUE INDICAN EL CODIGO DE TARJETA'
Me.Adodc3.Recordset.AddNew
'AÑADE DATOS DE INGRESO O SALIDA DEL USUARIO'
Me.Adodc3.Recordset(1) = Nombre.Text
Me.Adodc3.Recordset(2) = Vivienda.Text
Me.Adodc3.Recordset(3) = cod1.Text
Me.Adodc3.Recordset(4) = Date + Time
Me.Adodc3.Recordset(5) = numpuerta.Text
Me.Adodc3.Recordset.Update
End Sub
```

d. 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.

- ***Código***

```
Text11(0).LinkMode = 0
Text11(0).LinkTopic = "LNSDDE|Tesis_3.Subsystem 1.DevNV"
Text11(0).LinkItem = "LNS Network Interface.nvoAlrPuertared -t RAW"
Text11(0).LinkTimeout = 100
Text11(0).LinkMode = 1
If Text11(0).Text = “100;0 1” Then          ’Detecta si se ha producido una alarma’
MsgBox "Puerta 1 Abierta", vbOKOnly, "ALARMA!!!"
Me.Adodc4.Recordset.AddNew                  ‘Envío a base de datos’
Me.Adodc4.Recordset(1) = 1
Me.Adodc4.Recordset(2) = Date + Time
End If
```

2.3.7. Acceso técnico

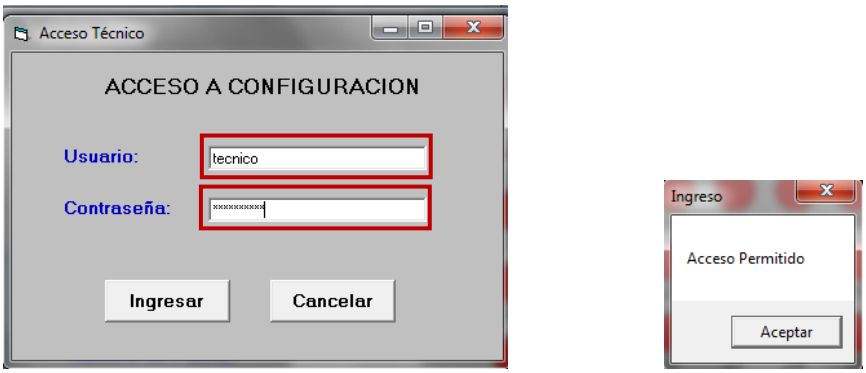


Figura. 2.24. Ingreso a Configuración

Al igual que el ingreso general del sistema en esta se hace una comparación similar, para dar el acceso a la configuración técnica. 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

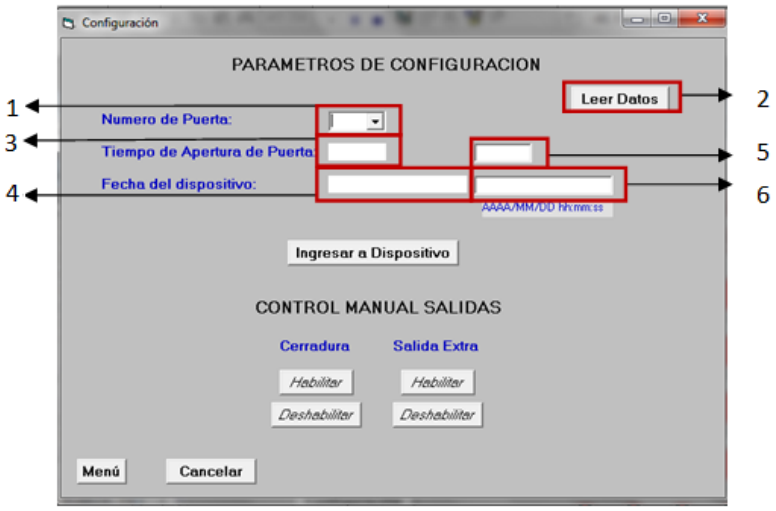


Figura. 2.25. Configuración

1. Nos permite seleccionar el dispositivo de una determinada puerta al que queremos configurar.
2. Después de haber elegido previamente al dispositivo de una puerta al que se requiere configurar se leen los datos del mismo.
3. En este espacio se muestra el valor del tiempo que la cerradura de la puerta permanece abierta.
4. En este espacio se muestra el valor de la fecha y hora actual del dispositivo.
5. En este espacio se puede reconfigurar el tiempo de apertura de la cerradura del dispositivo seleccionado.
6. En este espacio se puede reconfigurar la fecha y hora del dispositivo con el formato: AAAA/MM/DD hh:mm:ss.

Además consta de manejo manual de las salidas del dispositivo seleccionado, teniendo como opciones: *Habilitar* y *Deshabilitar* cada una de las ellas.

Consta de dos botones además de los principales que son:

- Menú: Dirige a la ventana menú
- Salir: Permite salir de la ventana Configuración

a. En la configuración técnica se puede hacer una modificación básica en la configuración de algún nodo en específico, que se selecciona en la pestaña **Numero de Puerta**; tal como la modificación del tiempo de apertura de la cerradura electromagnética y el reloj del nodo; atacando a la variable **UCP_Type_4[1]** y **nviFecha**; respectivamente. Esto se realiza para cada uno de los nodos que se encuentran instalados en el sistema.

Se tendrá acceso a los datos de configuración mencionados al seleccionar **Leer Datos.** Esto ayuda a conocer los datos actuales que tiene un nodo.

- ***Código***

```
Text1.Text = numpuerta2.Text
taperl.LinkMode = 0
taperl.LinkTopic = "LNSDDE|Tesis_3.Subsystem 1.DevCP"
horal.LinkMode = 0
horal.LinkTopic = "LNSDDE|Tesis_3.Subsystem 1.DevNV"
Select Case Text1.Text
Case 1
taperl.LinkItem = "Puerta1.UCP_Type_4[1]"
horal.LinkItem = "Puerta1.nvoReloj"
End Select
taperl.LinkTimeout = 100
taperl.LinkMode = 1
horal.LinkTimeout = 100
horal.LinkMode = 1
```

b. A continuación, se muestra como se ingresan nuevos datos de configuración al nodo seleccionado; mediante la selección de **Ingresar a Dispositivo**

- ***Código***

```
Text1.Text = numnodo.Text
Text2(0).LinkMode = 0
Text2(0).LinkTopic = "LNSDDE|Tesis_3.Subsystem 1.DevCP"
Text2(1).LinkMode = 0
Text2(1).LinkTopic = "LNSDDE|Tesis_3.Subsystem 1.DevNV"
Select Case Text1.Text
Case 1
Text2(0).LinkItem = "Puerta1.UCP_Type_4[1]"
Text2(1).LinkItem = "Puerta1.nviFecha"
```

End select
Text2(0).LinkTimeout = 100
Text2(0).LinkMode = 1
Text2(0).Text = taper.Text
Text2(0).LinkPoke
Text2(1).LinkTimeout = 100
Text2(1).LinkMode = 1
Text2(1).Text = Hora.Text
Text2(1).LinkPoke

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 de todos los nodos de control de accesos.

Para ello, se lee una variable 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.

- ***Código***

'Actuación si se produce un error
On Error GoTo errcom
'Leemos una varible del nodo de control 1
Text12(0).LinkMode = 0
Text12(0).LinkTopic = "LNSDDE|Tesis_3.Subsystem 1.DevNV"
Text12(0).LinkItem = "Puerta1.nvoEstCir1 -t RAW"
Text12(0).LinkTimeout = 100
Text12(0).LinkMode = 1

A continuación, el mensaje de error de comunicación que se muestra si este se produce:

- ***Código***

```
errcom:
Dim sedaño As Integer
sedaño = Err.Number          'Capta el número de error que se produce'
If sedaño Then
MsgBox "Error de comunicación con el nodo de la Torre A", vbOKOnly,
"Comuniacación Fallida"      'Mensaje de error'
Resume Next                  'Permite que siga la ejecución del programa'
End If
```

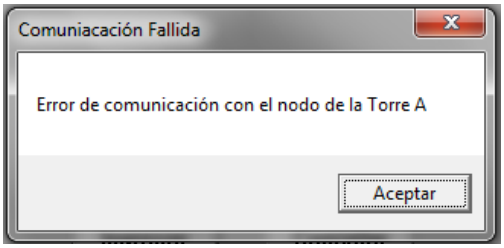


Figura. 2.26. Mensaje de error de comunicación

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.

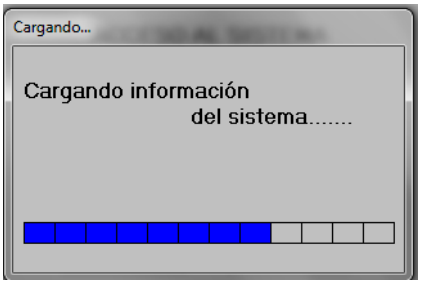


Figura. 2.27. Mensaje de error de comunicación

CAPITULO III

IMPLEMENTACIÓN

3.1. IMPLEMENTACIÓN DEL SOFTWARE DE CONTROL DE ACCESOS EN LAS OFICINAS DE ISDE – ECUADOR

3.1.1. Estructura Física para el Sistema de Control de Accesos

La oficina de ISDE - ECUADOR consta de un sistema de seguridad completo y de iluminación. El sistema posee un control de alarmas técnicas de intrusión, de humo, de fuego; como también posee un control de iluminación por escenas y control manual de cada circuito; para dar distintos ambientes de trabajo al lugar.

Para el sistema de seguridad es muy importante por su puesto el sistema de Control de Accesos que también ya se encuentra instalado en la oficina. Este sistema brinda una gran seguridad por el uso de tarjetas de proximidad que poseen un código único, haciendo prácticamente imposible copiar una de estas tarjetas y procurando que solo la persona a la que se le ha entregado un tarjeta tenga el acceso al sistema; a menos que esta se extravíe (la cual podrá ser eliminada del sistema).

El sistema de la oficina consta del siguiente panel como se ve en la Figura. 3.1, en la cual se observan los equipos o nodos que permiten el control de los

distintos sistemas mencionados anteriormente. Todos los nodos se comunican por el cable Lon, que permite la integridad de todo el sistema.

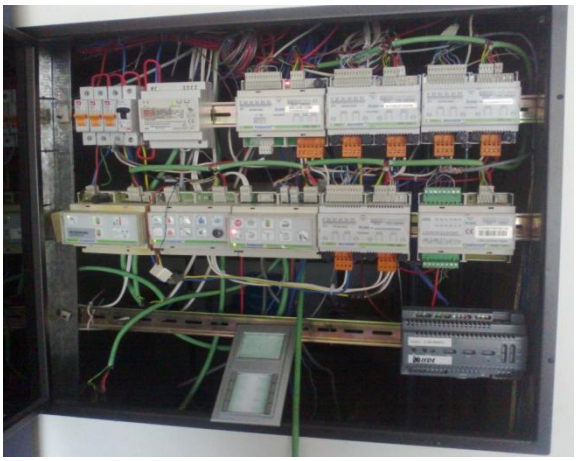


Figura. 3.1. Sistema Lonworks

a. Elementos del Sistema de Control de Accesos

El nodo que controla el Sistema de Control de Accesos es el de la Figura. 3.2, el Nodo INP-120.

Figura. 3.2. Nodo INP-120

La Figura. 3.3 y Figura. 3.4 muestran la cerradura electromagnética tanto su parte móvil como la estática. Siendo la parte estática, colocada en el marco de la puerta; la que se alimenta para imantarse y poder cerrar la puerta junto con la parte movible, que se recorre junto al movimiento de la puerta.

Figura. 3.3. Parte movible

Figura. 3.4. Parte estática

Para el ingreso a la oficina, en el exterior se encuentra el Lector de Proximidad ILP-200 como se observa en la Figura. 3.3, el cual permite la lectura del código de la tarjeta de proximidad; y que posteriormente si este está registrado en el sistema, se tendrá un acceso válido al lugar activando la cerradura electromagnética.

Figura. 3.5. Lectora ILP-200

Para la salida de la oficina, en el interior se encuentra un pulsador como se observa en la Figura. 3.4, que se conecta al nodo; el cual abre directamente la cerradura electromagnética.

Figura. 3.6. Pulsador

b. Conexión física

Vistos los elementos individuales de nuestro sistema de control de accesos, a continuación en la Figura. 3.6., se muestra la conexión de cada uno de dichos elementos al nodo INP-120 para que puedan funcionar integralmente en el sistema de control de accesos

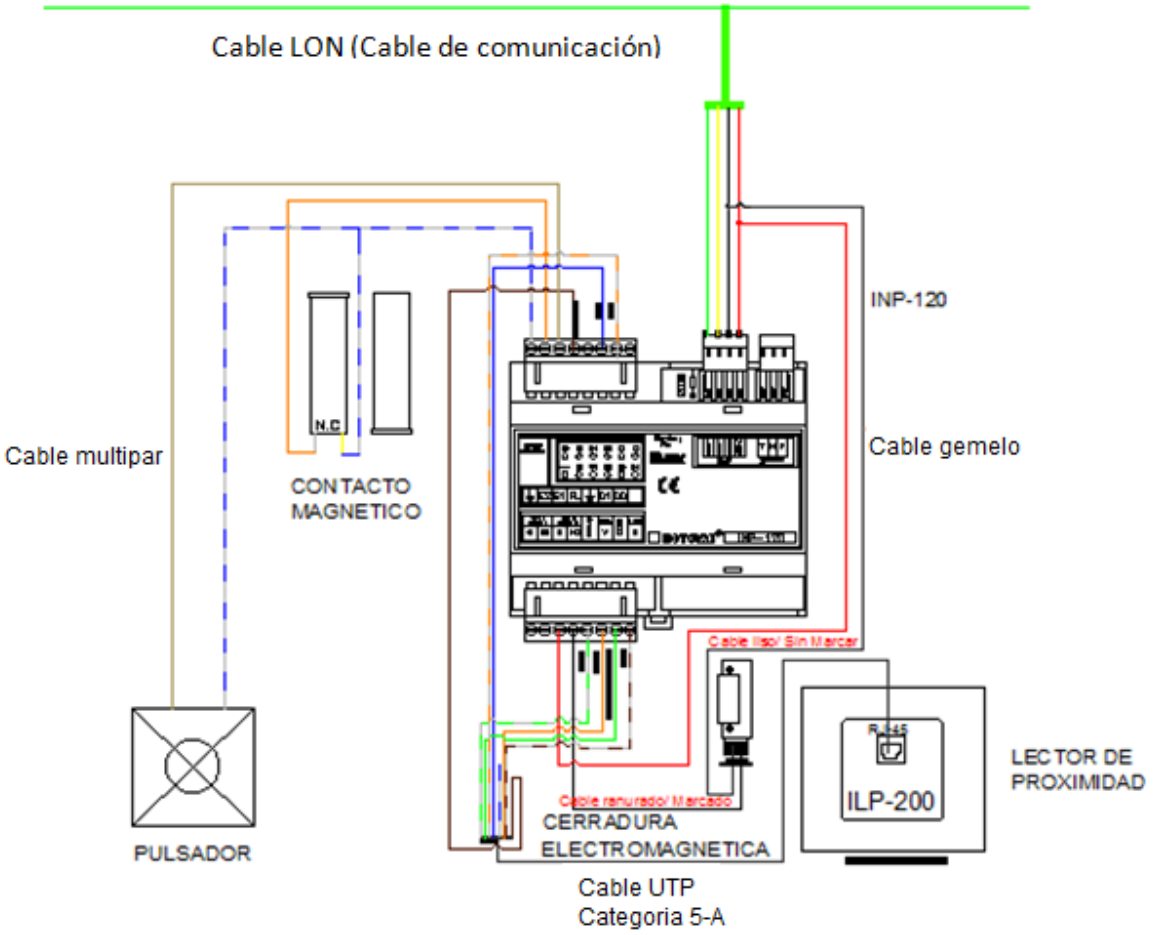


Figura. 3.7. Diagrama de conexiones

Para una mayor comprensión de la conexión de cada uno de los dispositivos al nodo INP-120, revisar el “Capítulo I”, desde la página 83 a 86.

3.2. PRUEBAS DE FUNCIONAMIENTO

Dado el sistema de Control de Accesos que se encuentra implementado en la oficina, se ve la necesidad de tener un mayor control de las personas que entran y salen de la oficina.

Si es cierto el sistema brinda seguridad para el acceso, el software desarrollado a implementar permite incrementar dicha seguridad; mediante una base de datos de todos los usuarios que tienen acceso al sistema y pudiendo así controlar que persona es la que tuvo acceso y la fecha en lo que lo realizó. Además de estas importantes características el software permite el ingreso de nuevas tarjetas al sistema de una manera más fácil y amigable.

3.2.1. Procesos de Funcionamiento

Para el correcto funcionamiento del software del Sistema de Control de Accesos, se debe tener una PC que actúe como un servidor; en la cual el software será instalado. Debe tener la característica de servidor ya que debe estar siempre encendido para que pueda registrar y/o monitorear cada acceso válido que se realice al recinto.

Instalado el Software se realizó las pruebas de funcionamiento del software junto al sistema físico del Control de Accesos.

3.2.1.1. Ingreso de Tarjetas

1. Se ingresa una Tarjeta Maestra (se da de alta a una tarjeta) y se comprueba que se obtenga un acceso válido al recinto. Además se observa en la base de datos de usuarios maestros que se encuentre registrada la nueva tarjeta ingresada. (Pág. 121)

2. Al momento que se produzca un acceso válido comprobar que este acceso se ha monitoreado y se ha registrado en la base de datos de accesos monitoreados. (Pág. 138)

3. Así mismo se realiza el procedimiento 1 y 2, pero en este caso con Tarjetas Condicionadas que se registra en la base de datos de usuarios condicionados y en le base de datos de accesos monitoreados.

3.2.1.2. Eliminación de Tarjetas

1. Se ingresa a la base de datos de usuarios maestros en donde se selecciona al usuario que se le quiere eliminar (o dar de baja), seleccionado el usuario elegido; se comprueba que ya no se tiene acceso válido al recinto. (Pág. 130)

2. Procedimiento similar al anterior se realiza para eliminar el usuario condicionado añadido al sistema , pero ingresando a la base de datos de usuarios condicionados.

3.2.1.3. Edición de Tarjetas

1. Se ingresa a la base de datos de usuarios maestros en donde se seleccionar al usuario que se requiere editar su información, a continuación la pantalla de edición aparecerá para poder cambiar los datos que sean requeridos. Se comprueba que el cambio a surtido efecto. (Pág. 130)

2. Procedimiento similar al anterior se realiza para editar el usuario condicionado añadido al sistema, pero ingresando a la base de datos de usuarios condicionados.

3.2.1.4. Habilitar y Deshabilitar Tarjetas

1. Ingresar a la pantalla de ingreso de tarjetas maestras, aquí se puede buscar a un usuario especifico guardado en la base de datos; al cual se le quiere deshabilitar su acceso al recinto momentáneamente. A continuación se selecciona la opción “Deshabilitar”. (Pág. 121)

2. Si dicha deshabilitación se la quiere retirar, se selecciona “Habilitar” y así el usuario queda nuevamente apto para acceder al recinto.

3.2.1.5. Configuración Técnica

1. Se ingresa a la pantalla de configuración técnica, para poder modificar si es necesario las configuraciones básicas del nodo/s del sistema de Control de Accesos, como son el tiempo de apertura de la cerradura electromagnética y la hora del nodo. (Pág. 152)

2. Además desde esta pantalla se prueba el manejo manual de las salidas 1 y 2 del nodo.

3.2.1.6. Alarmas y Comunicación

1. Cuando se produce un acceso válido al recinto, la puerta se deja intencionalmente abierta, asegurándose de que el tiempo que permanezca de esta manera sea mayor al tiempo configurado para que se produzca una alarma de puerta abierta en la ventana de monitoreo. (Pág. 144)

2. Al iniciarse el sistema se desconecta de forma intencional el nodo INP-120F, para de esta manera ver el error que produce el software cuando no detecta comunicación con un nodo específico. (Pág. 155)

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. 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.

4.2. RECOMENDACIONES

- 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.

- 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.

REFERENCIAS BIBLIOGRÁFICAS

- 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>, 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>, Control de accesos. [En línea].

- <http://www.taringa.net/posts/ciencia-educacion/9897059/Tecnologia-RFID.html>, Tecnologia RFID. [En línea].

- <http://es.wikipedia.org/wiki/RFID>, RFID. [En línea].

- <http://domotiva.wordpress.com/2010/09/03/la-tecnologia-lonworks/>, La tecnologia LONWORKS. [En línea].

- <http://www.forosdelweb.com/f69/fechas-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>, ActiveX Data Objects. [En línea].

- <http://social.msdn.microsoft.com/Forums/es-AR/winformses/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].