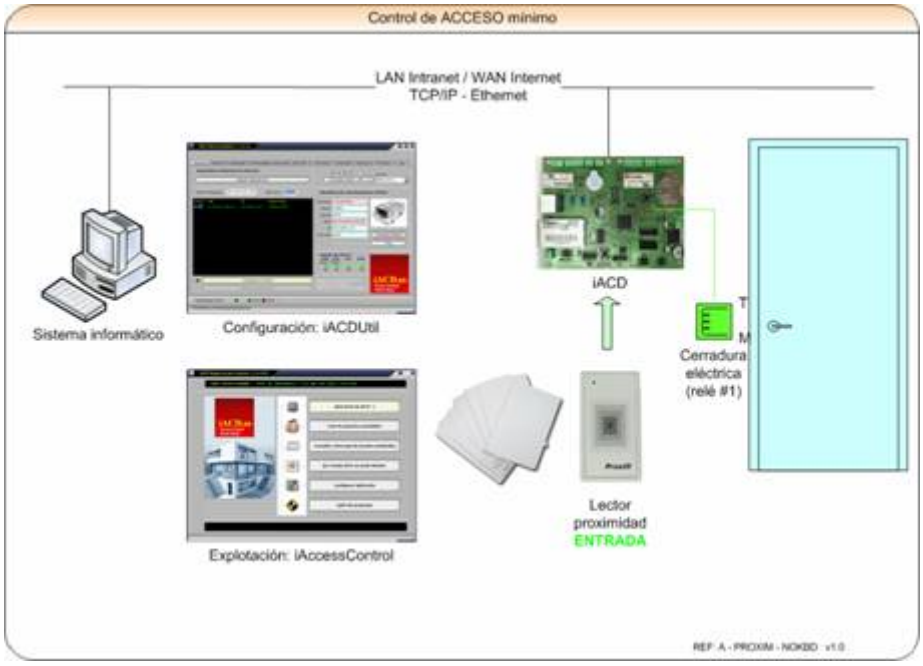
iACD

iACD es un dispositivo electrónico diseñado por **Indalo Security Systems** para su integración en sistemas de ***control de acceso y presencia*** . Para realizar estas labores de control precisa estar conectado a una serie de elementos en función de lo que se pretenda controlar.



En la imagen de la derecha puede ver un ejemplo de un sistemas de control de acceso con el mínimo de componentes posibles.

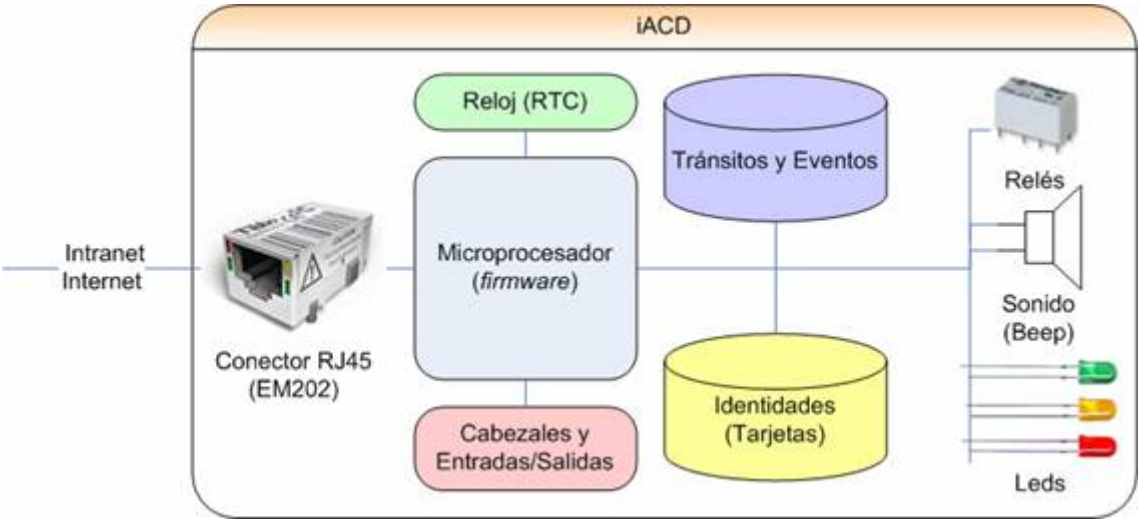
Los elementos empleados para este ejemplo se pueden generalizar para otras instalaciones y son:

- **Sistema informático**: Permite configurar y explotar el sistema.
  - **Configuración (iACDUtil):** Permite configurar los parámetros que rigen el comportamiento del dispositivo iACD tras su instalación
  - **Explotación (iAccessControl):** Es el software más sencillo que permite gestionar las tarjetas autorizadas en el dispositivo y recoger la información de los tránsitos y eventos producidos.
- **Lector**: Es necesario añadir uno o dos lectores para reconocer que se efectúa un tránsito. Estos lectores pueden ser de proximidad, de banda magnética, lector chip, Mifare, biométricos.

- **Actuador**: A los relés del dispositivo se puede conectar cualquier elemento de control de acceso (cerradura eléctrica, barrera, motor, torno, ?)

***NOTA**: Aunque no se especifique en el diagrama habrá que tener en cuenta la alimentación de los dispositivos y el cableado (de comunicaciones con el Sistema Informático, de alimentación y de control de los distintos elementos)*

Estructura interna



- **Conector RJ45 (EM202):** Permite la conexión a la red (TCP/IP sobre Ethernet) y su configuración en los aspectos de red (IP y puerto)
- **Microprocesador**: Ejecuta un programa denominado ***firmware***. Dependiendo del firmware que tenga cargado dispondrá de funcionalidades diferentes.
- **Reloj (Real Time Clock, RTC)** : Controla la hora del dispositivo y se mantiene activo gracias a la pila incorporada.
- **Cabezales y Entradas/Salidas**: Al dispositivo se le conectan cabezales (lectores) para identificar los accesos y además ciertas señales de entrada y salida.
- **Tránsitos y Eventos** : Existe una parte de la memoria destinada a almacenar los accesos (o intentos) y los eventos producidos. Esta memoria se puede y debe descargar periódicamente. Si se llena la memoria se empiezan a sobreescribir los tránsitos más antiguos.
- 

Identidades (Tarjetas): Otra parte de la memoria está destinada a gestionar las tarjetas habilitadas en el dispositivo.
- **Relés**: Existen dos relés que opcionalmente permiten controlar dispositivos externos vinculados a la lectura correcta de una tarjeta en un cabezal.
- **Sonido (Beep)**: Al efectuar una lectura en un cabezal se avisa mediante unos pitidos

del acceso permitido o denegado. La duración de estos pitidos es configurable.
- **Leds**: Existen unas luces indicadoras que igualmente informan del estado del dispositivos y de las operaciones efectuadas.

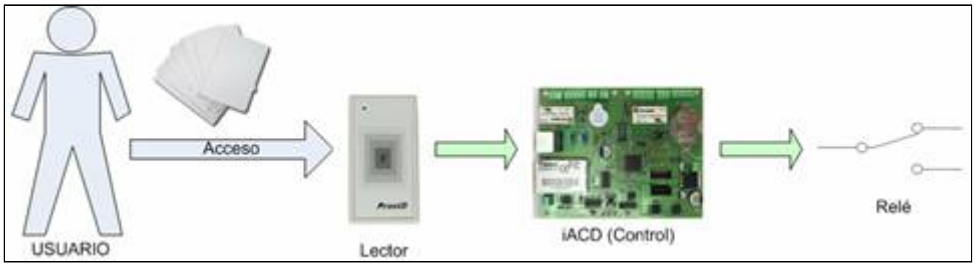
Comunicaciones

El sistema informático puede hablar con el dispositivo de dos formas posibles:

1. **UDP (puerto 65535)**: Un ejemplo típico es a la hora de buscar dispositivos, donde el servidor pregunta cuántos dispositivos hay y todos responden al mismo tiempo.
2. **TCP (puerto 3404)**: En este modo de comunicación el servidor inicia una conversación con un dispositivo iACD en concreto y le envía comandos a los que responde el dispositivo. Al finalizar se cierra la sesión.

Funcionamiento

Una vez configurado, el funcionamiento del dispositivo es sencillo:

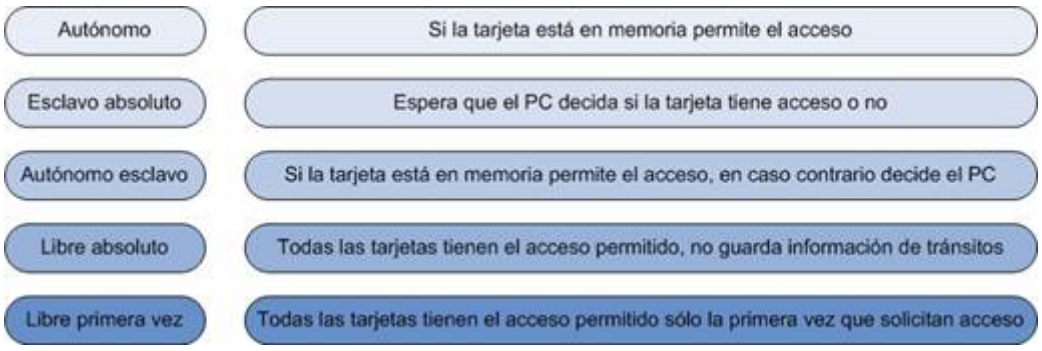


- **Identificación**: El usuario se identifica frente al lector (presentando una tarjeta, colocando su huella dactilar, ?) y este transmite un código al dispositivo iACD.
- **Tratamiento del código:** El código recibido es tratado convenientemente dependiendo de la configuración de los cabezales o lectores y de él se extrae opcionalmente un subconjunto de información.
- **Validación:** En base al Modo de Funcionamiento que tenga configurado, el dispositivo realiza la validación del ?usuario?.
- **Acción:** Una vez realizada la validación se procede a la memorización del tránsito, se notifica al usuario mediante pitidos y luces (leds) si el acceso está permitido o no y se activan los relés oportunos

Modos de funcionamiento

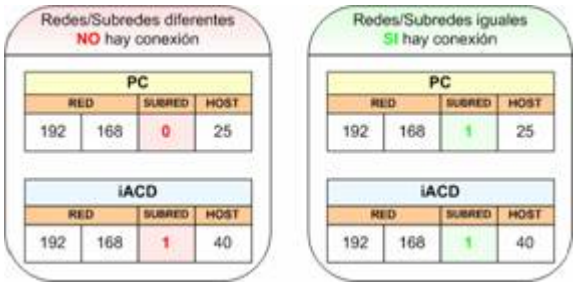
Dependiendo de qué tenga que controlar, el dispositivo dispone de diferentes modos de funcionamiento:

-



Autónomo: En este modo iACD sólo utiliza la información guardada en su propia memoria. Es decir, si el código a validar se encuentra en memoria se permite el acceso y si no está se deniega. Existe la posibilidad de coleccionar datos

- **Esclavo Absoluto**: Cada vez que se realiza una lectura, el dispositivo se queda a la espera de que el Servidor (software) le pregunte si tiene un intento de acceso.
    - Si el software responde *afirmativamente* se *permite* el acceso.
    - Si responde *negativamente* se *deniega* el acceso.
    - Si no se responde dentro de un tiempo que es configurable, también se *deniega* el acceso por*timeout*.
- **Autónomo Esclavo (*Autónomo + Esclavo Absoluto*)**: En este modo, una vez realizada la lectura se mira en la memoria de identidades.
    - Si la tarjeta está como autorizada se permite el acceso (modo *Autónomo*).
    - Si la tarjeta no figura como autorizada se espera la pregunta del Servidor y se responde en función de la respuesta recibida (modo *Esclavo Absoluto*)
- **Libre Absoluto**: Todas las lecturas dan como resultado acceso permitido. No se guarda información alguna de los tránsitos efectuados.
- **Libre Primera Vez**: Todas las lecturas dan como resultado acceso permitido la primera vez que se utiliza la tarjeta o identificación. En ese momento se guarda información de la tarjeta y el resto de las veces se deniega el acceso.

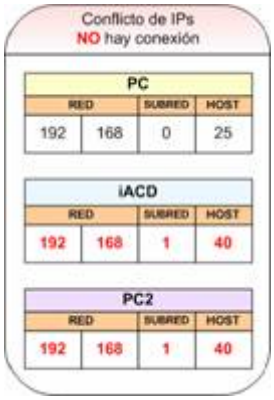


Conector RJ45 (EM202)

Parámetro	Valor
IP	192.168.1.40
Puerto TCP	3404
Puerto UDP	65535

El componente EM202 admite la configuración de algunos parámetros que permiten la comunicación entre el sistema informático y el dispositivo iACD.

Es muy importante configurar adecuadamente estos parámetros, en particular la IP ya que si no es adecuada para la red en la que va a trabajar, no será posible la conexión TCP.



En este ejemplo el PC y la placa iACD están bien configurados, pero existe un segundo ordenador que tiene la misma IP que la iACD. Esto impide que ambos dispositivos (iACD y PC2) funcionen correctamente.

***NOTA**: Ante cualquier duda consulte con el administrador de la red donde vaya a instalar dispositivos iACD o consulte un manual sobre administración de redes.*

Microprocesador

Es componente principal del dispositivo y su funcionamiento está controlado por un programa llamado*firmware* que está ejecutando en todo momento. Dependiendo de la versión del firmware que tenga cargada tendrá disponibles unas opciones u otras.

En concreto existen diferentes versiones de firmware para permitir la conexión de cabezales (lectores) con diferentes tecnologías de comunicación.

Cabezales (Lectores)

TIPOS DE CABEZAL / LECTOR
Plano. Mapa de bits
Data & Clock, ABA Track 2
Xtreme Secure Format, XSF
Wiegand 26
Wiegand 32
Wiegand 34
TTL Serie

El dispositivo iACD admite la utilización de uno o dos cabezales lectores simultáneamente. Los cabezales se utilizan para identificar a las personas y/o vehículos utilizando tecnologías muy diversas. Lo más importante a la hora de conectar los cabezales es tener en cuenta la tecnología de comunicación con el dispositivo electrónico. En la figura de la derecha se muestran algunos de los tipos los tipos admitidos.

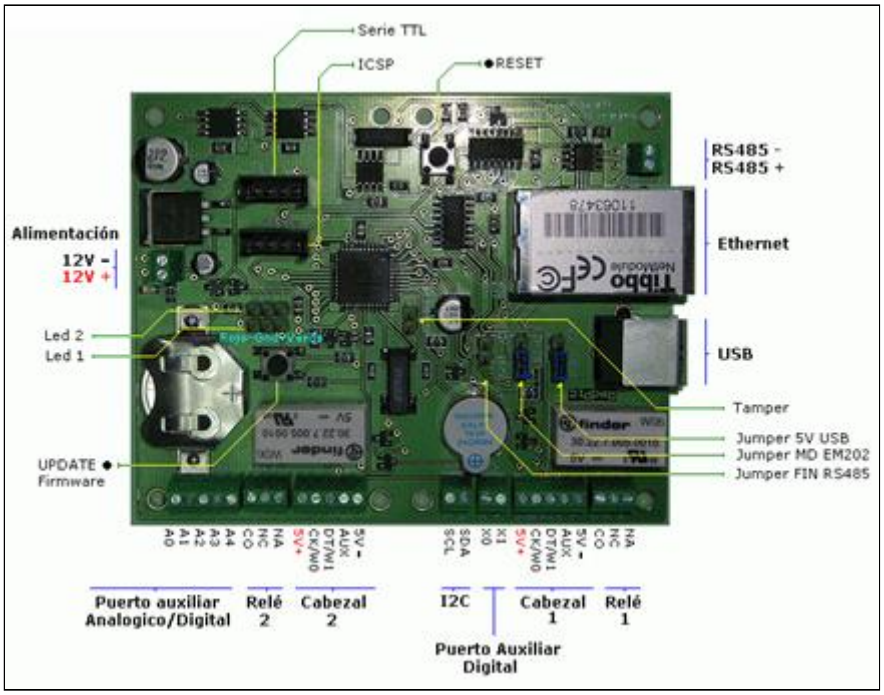
***NOTA**: El dispositivo iACD necesita tener cargada la versión del firmware que permite hablar con un tipo de cabezal concreto.*

Para iACD sólo importa el tipo de comunicación con el lector y es independiente de la tecnología empleada para la identificación:

- Banda magnética (alta y baja coercitividad)
- Proximidad 125 Khz (EM - ISO EM4102, TEMIC - ISO T5557)
- Proximidad 13.56 MHz (ISO MifareS50)
- Lector chip (múltiples variantes)
- Biométricos (huella dactilar, ?)

Reloj (RTC)

El reloj de tiempo real o Real Time Clock (RTC) permite saber a la iACD en todo momento la hora que es. Esta hora se asocia a cada tránsito o evento producido y se devuelve a la hora de descargar la información. Durante la instalación y configuración es necesario asegurar la puesta en hora del reloj para que la información sea útil. El reloj lleva una pila que le permite seguir en marcha en ausencia de alimentación.



Entradas/Salidas

Además de la conexión para los 2 cabezales de lectura independientes, el dispositivo cuenta con:

- 2 relés de salida
- 1 señal de tamper
- 6 entradas/salidas analógico/digitales
- 1 buzzer
- 2 leds tricolor

Conexiones de la placa iACD v1.0.4

Las conexiones que se emplean más comunmente son:

- **Cabezales (Lectores)**: Para realizar la identificación de los usuarios
- **Relés**: Permiten activar mecanismos (cerraduras eléctricas, tornos, barreras, ?) cada vez que se realiza un acceso correcto
- **Leds**: Muestran Las indicaciones luminosas de acceso permitido o acceso denegado
- **Tamper**: Permite detectar si han abierto la caja donde está instalado el dispositivo
- **Volumétrico**: Detecta si se produce una alarma por intrusión
- **Sensor de puerta**: Permite detectar si se realiza o no un acceso una vez autorizado, si se dejan la puerta abierta tras el acceso o si fuerzan la puerta sin haber acceso

***NOTA**: No se menciona, pero es evidente, que es necesario alimentar la placa con 12V y conectarla a una red Ethernet. Además existe la posibilidad de conectarse vía USB para actuaciones especiales bajo la guía del servicio técnico epecializado.*

Tránsitos y Eventos

Gran parte de la memoria de 512Kb está destinada a almacenar los accesos realizados a través de los lectores y los eventos producidos sobre los sensores.

Los tránsitos se componen básicamente de los siguientes datos:

- 

Fecha y hora
- Identidad o código de la tarjeta
- Número del cabezal: Permite identificar si es entrada o salida

Los eventos se componen de:

- 

Fecha y hora
- Fuente del evento (tamper, puerta, volumétrico, ?)
- Estado: abierto o cerrado

La memoria de tránsitos y eventos está organizada como una cola circular. Si los tránsitos (T1, T2, ?, Tn) o eventos, no se descargan periódicamente, la memoria se llena. Al llenarse, los tránsitos nuevos empiezan a escribirse encima de los más antiguos. Cada vez que se descargan o sincronizan los tránsitos, la memoria se queda vacía.

Identidades (tarjetas)

Las identidades reciben ese nombre debido a que pueden representar tanto tarjetas que

identifican a usuarios, como códigos asociados a datos biométricos, por ejemplo huellas dactilares. La información que lleva asociada una identidad es la siguiente:

Identidad						
Código	Cabezales	Revisión	Tipo	Inicio validez	Fin validez	APB
123456789012345	1	1	0	dd/MM/yyyy hh:mm:ss	dd/MM/yyyy hh:mm:ss	No

- **Código**: Es el código de la tarjeta o del usuario. Dependiendo de cómo se configuren los cabezales así será el código, por ejemplo de 10 caracteres.
- **Cabezales**: Indica a qué cabezales tiene acceso una identidad. Puede tener acceso a un cabezal, al otro o a los dos a la vez.
- **Revisión**: En las tarjetas en las que se puede grabar información (banda magnética, lector chip, ?) es posible controlar la versión de la tarjeta. Si alguien pierde la tarjeta le podemos reemitir otra exactamente igual pero con un número de revisión diferente para distinguirla de la anterior.
- **Tipo**: Indica el tipo de tarjeta.
- **Inicio y fin de validez**: Son fechas que indican el periodo de validez de la tarjeta en el dispositivo.
- **APB**: Indica si la identidad se ve afectada por el AntiPassBack (si una persona ya está dentro no puede volver a entrar hasta que realice una salida).

***NOTA**: Es importante resaltar que para que muchos de estos datos se tengan en cuenta en el dispositivo, es necesario configurar convenientemente los cabezales y,* ***en la mayoría de los casos basta con especificar el código de la identificación y los cabezales a los que tiene acceso**.*
