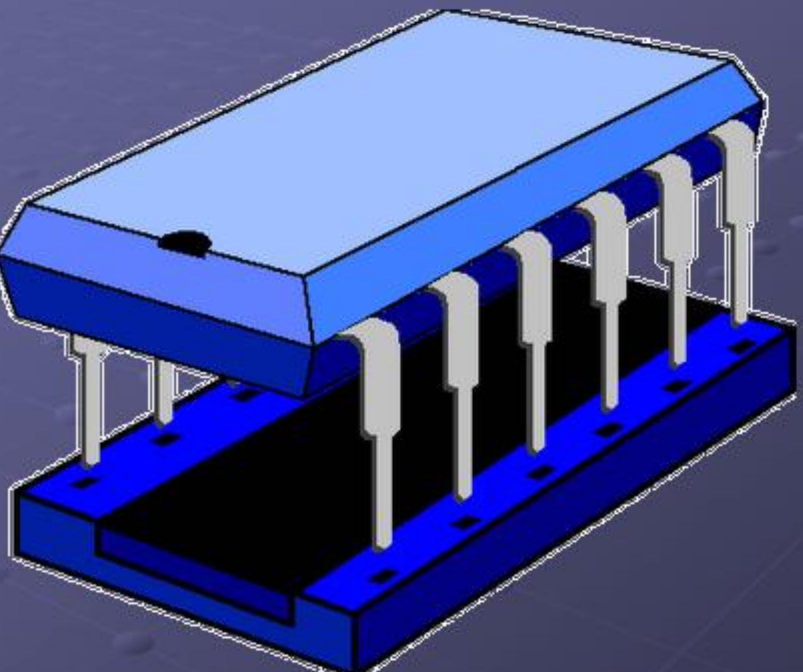
MICROCONTROLADORES AVANZADOS.



Ing. Carlos Valdivieso.

SISTEMA DE SEGURIDAD DE EQUIPOS DE LABORATORIO

Juan Domínguez
Miguel Iturralde

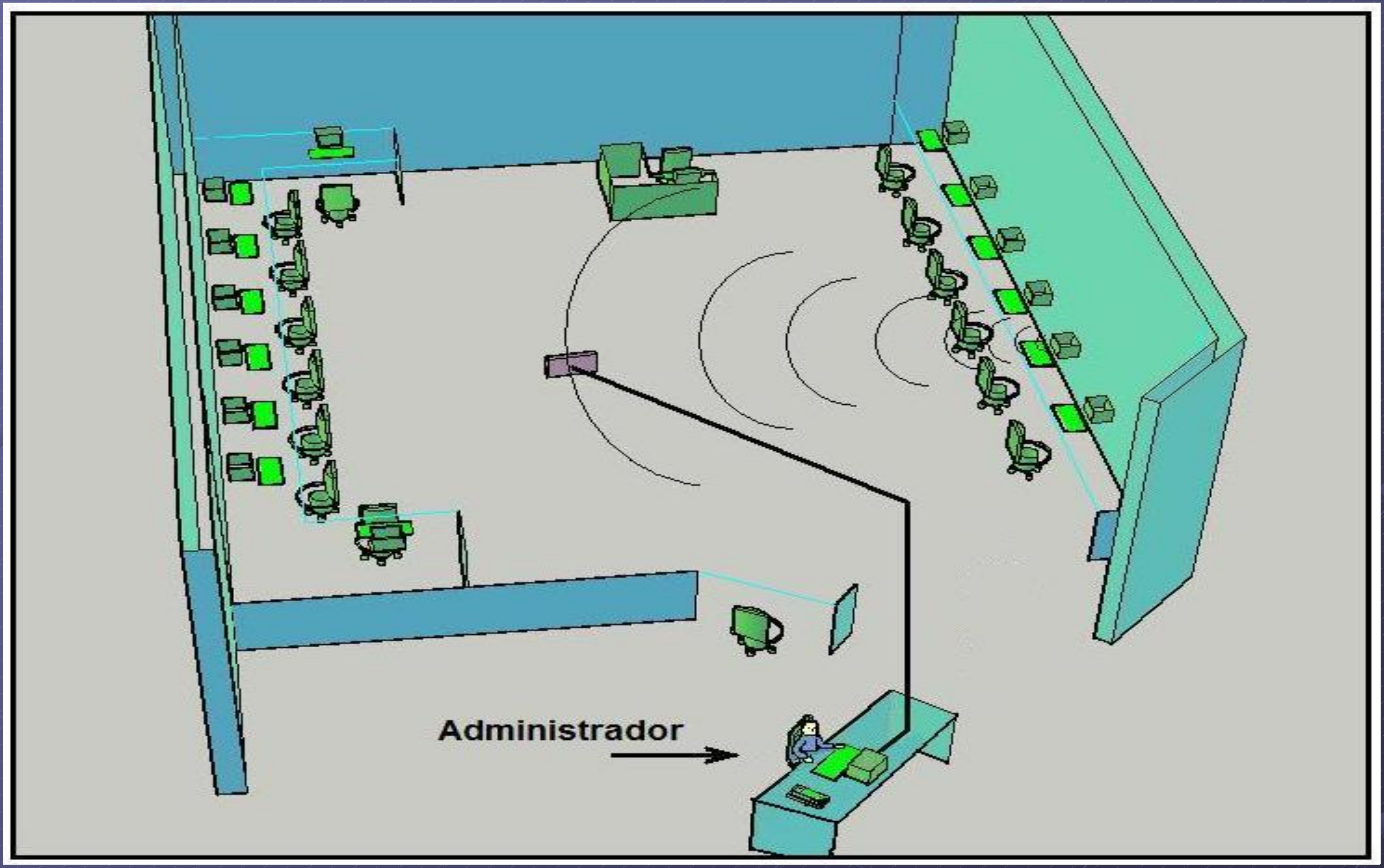
DESCRIPCION GENERAL DEL SISTEMA.

- Garantizar la permanencia de los equipos en las inmediaciones del laboratorio.
- Proporcionar una interfaz amigable con el usuario.
- Fácil instalación

ESTRATEGIA IMPLEMENTADA.

- Sistema de comunicación inalámbrico que permite el monitoreo de los equipos.
- Compuesto por un transmisor y un receptor de señales de Radiofrecuencia.
- El transmisor se puede insertar en los equipos cuya seguridad se desea garantizar.

ESTRATEGIA IMPLEMENTADA.



ESTRATEGIA IMPLEMENTADA.

- El Administrador podrá monitorear el sistema a través de MySQL y LabVIEW.
- Si la etiqueta sale del área de cobertura del Lector, el sistema emite una señal de alerta.
- Gracias al ID del tag se podrá saber cual equipo y en que momento abandonó el laboratorio.

LIMITACIONES DEL PROYECTO.

- Acceso a la tecnología requerida.
- Costo.
- Interferencia.
- Cobertura.

LIMITACIONES DEL PROYECTO.

- Debido a restricciones presupuestarias no nos es posible implementar a escala real
- Utilizaremos RFID de tipo pasivo.
- Dará la señal de alerta al detectar la señal del tag, en lugar de alertar ante la ausencia de la señal.

LIMITACIONES DEL PROYECTO.

- Se recomienda utilizar un RFID de tipo activo. Preferiblemente el kimaldi SYRD 2451N
- Cobertura entre 10 y 12 m.
- Opera a 2.4 GHz.
- Capacidad de lectura multi tag.
- Costo €767.

MODULO RFID READER #28140.

- Identifica Tags RFID de tipo pasivos.
- Cada Tag tiene un ID único que puede ser leído por el RFID Reader.
- Opera a 125 KHz.
- Costo $65

MODULO RFID READER #28140.

Tiene cuatro terminales .

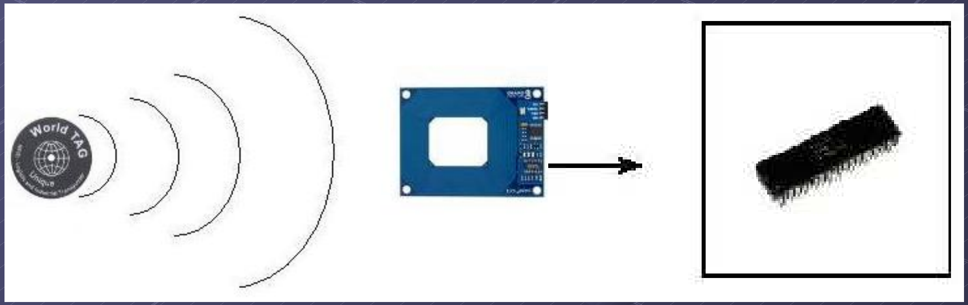
- VCC
- Enable
- Sout
- GND

MODULO ET-MINI ENC28J60.

- Permite la comunicación entre un microcontrolador y una red Ethernet.
- Soporta el estándar de comunicación IEEE 802.3 y trabaja utilizando un bus SPI.

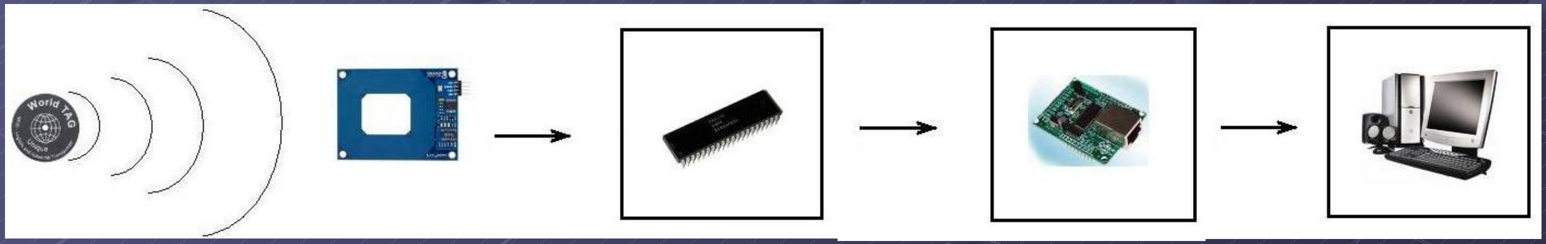
ANALISIS DEL DISEÑO PROPUESTO.

- El primer bloque está conformado por el módulo RFID que permite la adquisición y digitalización de los datos.
- El siguiente bloque es el conformado por el PIC18F4520, que permite el procesamiento de los datos

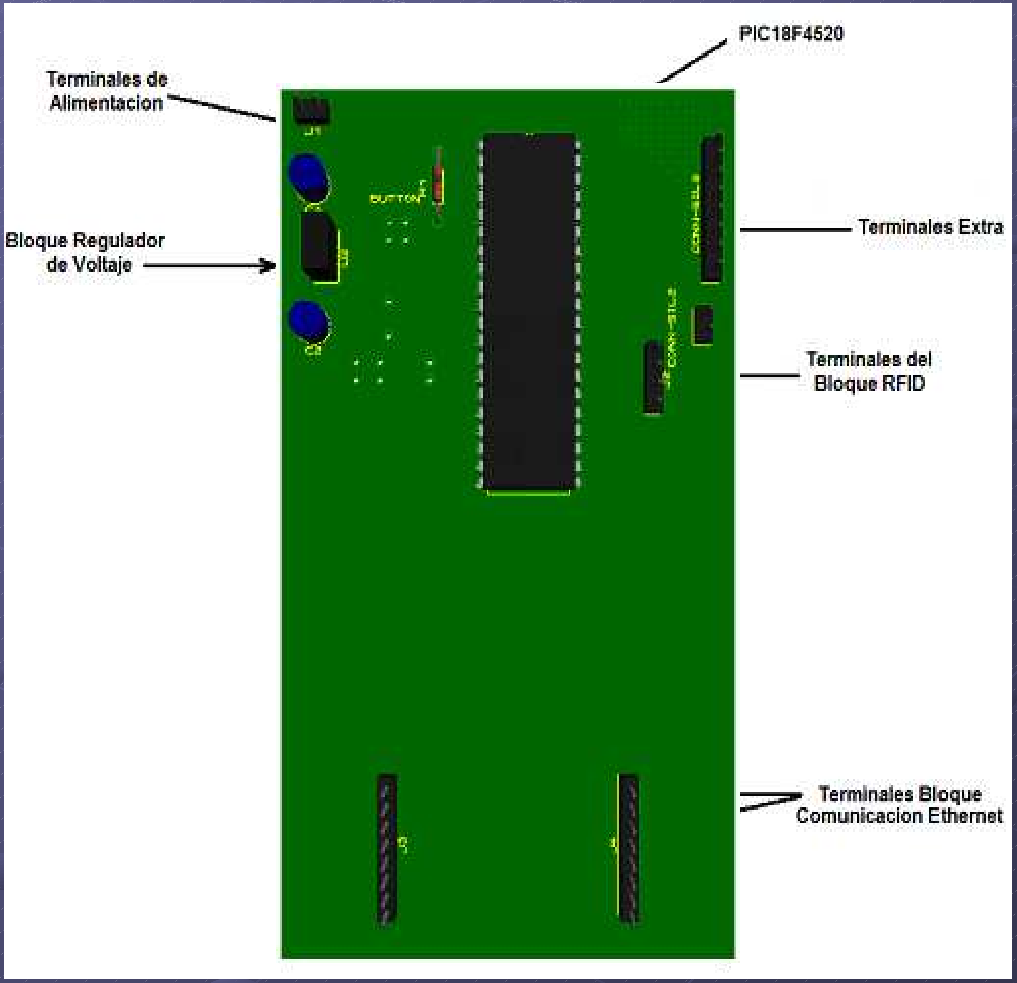


ANALISIS DEL DISEÑO PROPUESTO.

- El bloque de comunicación Ethernet envía los datos adquiridos por el sensor a través de la red hacia el host del administrador del laboratorio
- Finalmente los datos son procesados por el host del administrador.



ANALISIS DEL DISEÑO PROPUESTO.

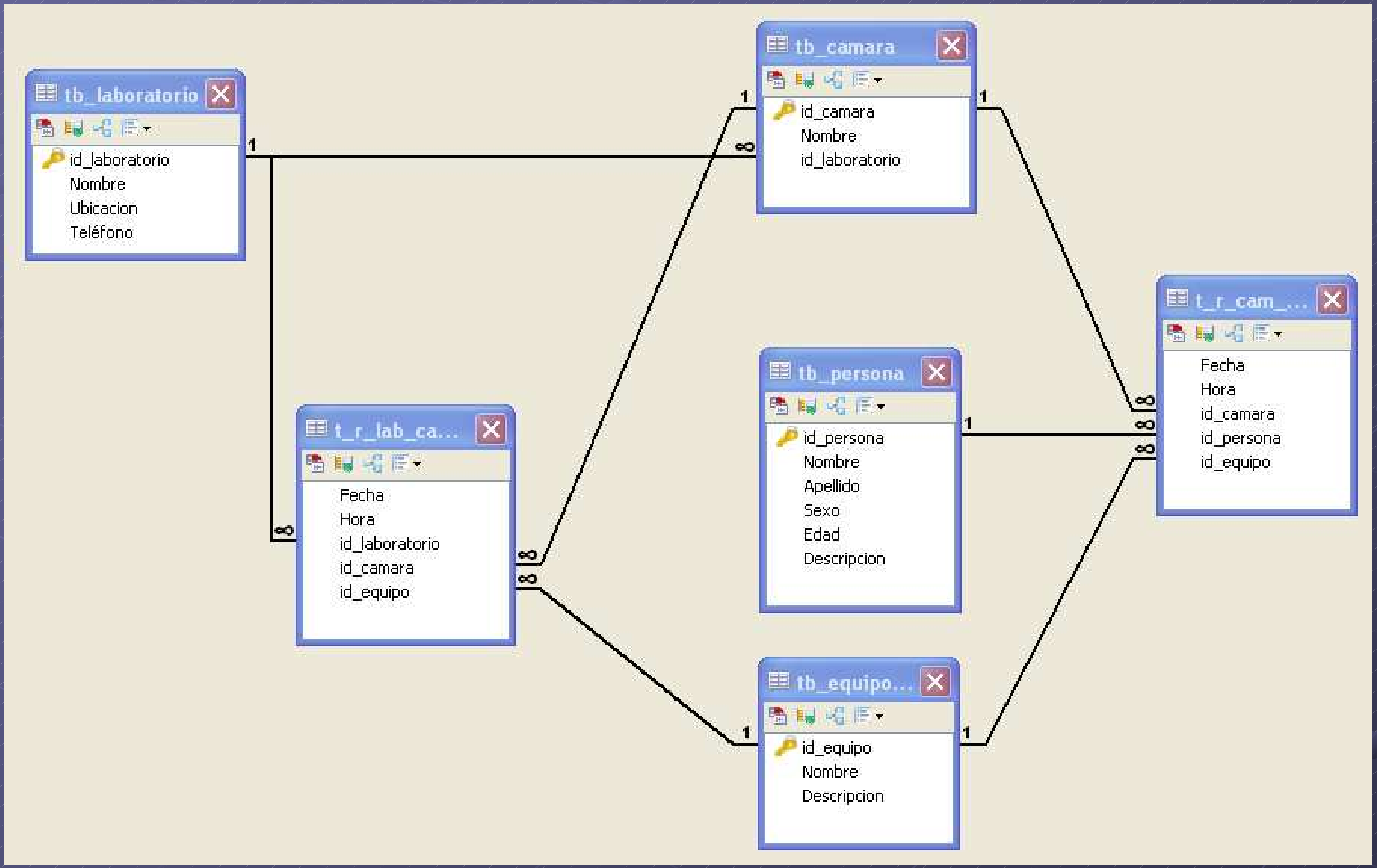


ANALISIS DEL CODIGO EN MIKROBASIC.

```
  spi_init()
  spi_ethernet_init(portc,0,portc,1,mymacaddr,myipaddr,1)
  IpAddr[0] = 192
  IpAddr[1] = 168
  IpAddr[2] = 46
  IpAddr[3] = 209

  Usart_Init(2400)
  cc = chr(13)
  bytetostr(cc,delim)
' delim =  "  "
   txt=""
   while true
   if Usart_Data_Ready = 1 then
       Usart_Read_text(tag, delim)
       delay_ms(1000)
       spi_ethernet_sendUDP(IpAddr, 10001, 4000, @tag, Strlen(tag))
       delay_ms(1000)
    end if
        spi_ethernet_dopacket()
  wend
end.
```

DISEÑO DE LA BASE DE DATOS



MANEJO Y PUESTA A PRUEBA.

CONCLUSIONES Y RECOMENDACIONES.

- El Sistema proporciona una completa seguridad tanto proactiva como reactiva, para cada uno de los equipos del laboratorio, tanto de día como de noche. Esta es una de las principales diferencias respecto a otros sistemas, ya que el módulo RFDI puede trabajar al 100% de sus posibilidades en horario diurno, cuando los usuarios están utilizando sus equipos del laboratorio.

- El sistema puede complementarse e integrarse con los sistemas de seguridad perimetrales actuales, como las cámaras de seguridad o Sistemas CCTV, sensores, Sistemas de control de acceso, entre otros; aportando una inmejorable prevención de los posibles riesgos que pueden padecer los equipos del laboratorio.

CONCLUSIONES Y RECOMENDACIONES.

- Para el manejo del sistema de seguridad se ha utilizado el software Labview 8.5 que permite al usuario tener una interfase amistosa de tipo gráfica con el cual se puede tener un mayor control de los equipos que se encuentran dentro del laboratorio.
- Es recomendable que las etiquetas se coloquen en lugares no visibles para el usuario.
- Existe el riesgo de que se modifique fraudulentamente la información contenida en la etiqueta RFID mediante dispositivos portátiles, como PDAs o similares; esto podría suceder si se utilizan tarjetas electrónicas RFID activas, que tienen la capacidad de cambiar su identificación.

GRACIAS POR SU ATENCION.