

# PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

## FACULTAD DE CIENCIAS E INGENIERÍA



PONTIFICIA  
**UNIVERSIDAD**  
**CATÓLICA**  
DEL PERÚ

### DISEÑO E IMPLEMENTACIÓN DE UN EQUIPO DE VOTO ELECTRÓNICO

Tesis para optar el Título de Ingeniero Electrónico, que presenta el bachiller:

**Marco Antonio Alberto Urday Chávez**

ASESOR: Ing. Javier Chang Fu

Lima, Noviembre de 2012

## RESUMEN

Los procesos electorales se modernizan al utilizar el voto electrónico como una herramienta que incorpora las tecnologías de información y comunicación a la jornada electoral. El acto de votar puede ser manual o electrónico, en ambos casos puede ser presencial o no presencial. En la modalidad de voto electrónico presencial, el ciudadano va al local de votación a emitir su voto en un equipo electrónico que le permite manifestar su voluntad electoral.

El presente trabajo tiene como objetivo el diseño y la implementación de un prototipo funcional de equipo de voto electrónico presencial, que permita al elector ejercer su derecho de elegir. El equipo permite seleccionar una agrupación política o un candidato, de la lista mostrada en un papel impreso, mediante la acción del elector al tocar y presionar con el dedo, sobre una lámina táctil transparente. La selección ocurre al observar la luz de color rojo de un diodo emisor de luz, al costado de la imagen del símbolo de la agrupación política. El equipo es habilitado para permitir ejecutar un solo voto por elector, mediante una llave electrónica conectada al equipo. En la conexión de la llave se implementa un canal de comunicación con un protocolo serial. Los resultados de la votación son almacenados en la llave electrónica y presentados al final de la votación, mediante una aplicación de software mostrada en una computadora personal.

## ÍNDICE GENERAL

<b>1</b>	<b>ANÁLISIS DEL CONTEXTO .....</b>	<b>1</b>
1.1	VOTO ELECTRÓNICO .....	1
1.2	OBJETIVOS DEL VOTO ELECTRÓNICO.....	1
1.3	CLASIFICACIÓN DEL VOTO ELECTRÓNICO.....	1
1.4	ESTADO DE LA TÉCNICA.....	1
1.5	SOLUCIÓN DE VOTO ELECTRÓNICO PRESENCIAL EN EL PERÚ .....	4
1.6	PROPUESTA DE EQUIPO DE VOTO ELECTRÓNICO PRESENCIAL .....	6
1.7	OBJETIVOS .....	7
<b>2</b>	<b>DISEÑO E IMPLEMENTACIÓN DEL HARDWARE.....</b>	<b>8</b>
2.1	PRINCIPALES REQUERIMIENTOS.....	8
2.2	COMPONENTES DE LA SOLUCIÓN.....	9
2.2.1	<i>Lámina Táctil .....</i>	<i>11</i>
	<i>Coordenadas del punto de presión.....</i>	<i>12</i>
2.2.2	<i>Microcontrolador A.....</i>	<i>14</i>
	<i>Requerimientos del Microcontrolador .....</i>	<i>14</i>
	<i>Selección del microcontrolador .....</i>	<i>14</i>
	<i>Convertor Análogo Digital.....</i>	<i>16</i>
2.2.3	<i>Dispositivo Visual.....</i>	<i>17</i>
2.2.4	<i>Generador de Sonido .....</i>	<i>18</i>
2.2.5	<i>Microcontrolador B.....</i>	<i>20</i>
	<i>Requerimientos del Microcontrolador .....</i>	<i>20</i>
	<i>Selección del microcontrolador .....</i>	<i>20</i>
2.2.6	<i>Computadora Personal.....</i>	<i>20</i>
2.2.7	<i>Fuente de Voltaje.....</i>	<i>20</i>
2.2.8	<i>Fuente de Energía Eléctrica .....</i>	<i>21</i>
	<i>Tiempo de autonomía de energía eléctrica.....</i>	<i>22</i>
2.3	TARJETA CONTROLADORA .....	24
2.4	TARJETA LLAVE DE HABILITACIÓN.....	26
<b>3</b>	<b>DISEÑO E IMPLEMENTACIÓN DEL FIRMWARE .....</b>	<b>28</b>
3.1	OBTENCIÓN DE LAS COORDENADAS (x, y) .....	28
3.2	CONFIGURACIÓN DE LA CÉDULA DE VOTACIÓN.....	30
3.3	COMUNICACIÓN EQUIPO – LLAVE.....	30
3.4	PROTOCOLO DE COMUNICACIÓN SOBRE UN PIN .....	31
<b>4</b>	<b>IMPLEMENTACIÓN DEL SOFTWARE.....</b>	<b>43</b>
4.1	ACTIVACIÓN DE LA LLAVE HABILITADORA .....	43
4.2	APLICACIÓN DE VOTO ELECTRÓNICO.....	43
<b>5</b>	<b>INTEGRACIÓN E IMPLEMENTACIÓN DEL PROTOTIPO .....</b>	<b>46</b>
5.1	PROTOTIPO .....	46
5.2	COSTOS DE LA IMPLEMENTACIÓN DEL PROTOTIPO .....	47

<b>6</b>	<b>SEGURIDAD DE LA INFORMACIÓN .....</b>	<b>51</b>
6.1	CARACTERÍSTICAS DE LA SEGURIDAD DE LA INFORMACIÓN.....	51
6.2	ANÁLISIS DE RIESGO DEL EQUIPO DE VOTO ELECTRÓNICO .....	52
6.3	CRIPTOGRAFÍA .....	52
	<b>CONCLUSIONES .....</b>	<b>56</b>
	<b>RECOMENDACIONES .....</b>	<b>56</b>
	<b>BIBLIOGRAFÍA .....</b>	<b>57</b>
	<b>ANEXOS .....</b>	<b>61</b>



## 1 ANÁLISIS DEL CONTEXTO

### 1.1 Voto electrónico

¿Qué es el voto electrónico?

Es una forma de expresión secreta de una preferencia ante una opción, basada en medios electrónicos que se diferencia del método tradicional por la utilización de equipos electrónicos y programas informáticos que permiten automatizar los procesos de comprobación de la identidad del elector, emisión del voto, conteo de votos y emisión de reportes de resultados [1].

### 1.2 Objetivos del voto electrónico

- Rapidez en la obtención y publicación de los resultados de la jornada electoral, y
- Sencillez en la ejecución de los procesos de comprobación de la identidad del elector, emisión del voto, conteo de votos y emisión de reportes de resultados [2].

### 1.3 Clasificación del Voto electrónico

La tipificación más sencilla es la que se produce al dividir los procesos de votación en presenciales y no-presenciales. Se dice que el proceso de votación es presencial cuando se identifica manualmente al elector, autorizándolo a utilizar una máquina dispuesta en un lugar específico (local de votación).

Por el contrario, cuando el voto es ejercido no-presencialmente, es decir, de forma remota, a través de Internet (votación telemática), el sistema lo hace todo (identificar y enviar el voto) y, probablemente, con independencia del dispositivo (computador personal o equipamiento equivalente). Por ende, en este caso, el equipo no es específico [3].

### 1.4 Estado de la Técnica

En muchos países del mundo se ha considerado el uso del voto electrónico. En algunos países se realizan pruebas y en otros se utiliza de forma vinculante.

Entre los países que han implementado el voto electrónico presencial en el 100% de sus mesas electorales destaca:

### Brasil

Ha implementado desde el año 2000, el voto electrónico presencial en el 100% de sus mesas electorales, con una participación de 109 millones de electores en el año 2000 y 135.8 millones de electores en el año 2010 [22]. Utiliza una urna electrónica compuesta por un terminal de mesa y un terminal de elector [23]. En el terminal de mesa se identifica al elector a través de la huella dactilar o digitando los números de su documento de identidad, con lo cual se habilita el terminal del elector para realizar un voto, el elector digita los números de sus opciones políticas y verifica en la pantalla sus selecciones, de estar de acuerdo confirma su voto. Se imprime un comprobante del voto, el cual no es accesible al elector y que sirve para una auditoría posterior a la jornada electoral. El peso del equipo de voto electrónico no es mayor a 10 Kg. En la figura N° 1.1 se muestra el equipo de voto electrónico utilizado actualmente en Brasil.



Figura 1.1 Equipo de voto electrónico utilizado en Brasil

Las características del hardware del equipo de voto electrónico de Brasil se indican a continuación.

El terminal del elector posee los siguientes componentes:

- Gabinete
- Placa madre
- Procesador compatible con X86 de 32 bits
- RAM socket DDR
- Reloj interno
- Generador de sonidos
- Controlador de video VGA

- Controlador SATA , ATA 2
- Unidades de almacenamiento
- Teclado numérico
- Display LCD 10" 800x600
- Fuente de alimentación
- Alimentación externa con tensión de entrada variando entre 90 a 220 Vac
- Alimentación interna con batería de 12 voltios dc
- Batería interna
- Diodos emisores de luz
- Mecanismo de impresión

El terminal de mesa posee los siguientes componentes:

- Gabinete
- Display alfanumérico
- Display gráfico 2" , 240x320 colores
- Teclado numérico
- Diodos emisores de luz
- Dispositivo de lectura de huellas dactilares
- Dispositivo de lectura y grabación de tarjetas inteligentes
- Generador de sonidos
- Puerto USB 2.0

## Venezuela

Implementó desde el año 2009 el voto electrónico presencial en el 100% de sus mesas electorales. En el año 2010, la población electoral para las elecciones parlamentarias fue de 17'575,975 [24]. Se usan equipos fabricados por la empresa Smartmatic, cuyos modelos utilizados son SAES 3000, SAES 3300 y SAES 4000. El modelo SAES 4000 [25] tiene las siguientes características:

- Monitor VGA de 10.4 pulgadas
- Pantalla táctil resistiva
- Microprocesador Celeron 600Mhz
- Memoria RAM máxima de 1 GB
- Dispositivo de almacenamiento (memoria interna de 256 MB, un slot para compact flash)
- Impresora térmica con ancho de papel de 8 cm.

- 6 puertos USB 2.0
- Un puerto PS2 para la boleta electrónica
- Un puerto de red RJ-45
- Peso del equipo igual a 5.9 Kg.
- Alimentación externa con tensión de entrada variando entre 100 a 240 Vac

Accesorios:

- Boletas electrónicas (configuración de la lista de candidatos en sistemas digitales)
- Batería externa
- Maleta protectora

Opciones de activación:

- Botón de control remoto
- Activador de tarjeta Smartcard
- Dispositivo Captahuella

En la figura N° 1.2 se muestra el equipo de voto electrónico utilizado actualmente en Venezuela.



Figura 1.2. Equipo de voto electrónico utilizado en Venezuela

### 1.5 Solución de voto electrónico presencial en el Perú

Actualmente la Oficina Nacional de Procesos Electorales (ONPE) posee una solución tecnológica para voto electrónico presencial, la cual se encuentra en la etapa de prototipo. Esta solución fue diseñada por la Pontificia Universidad Católica del Perú [4] e implementada por la Universidad Nacional Mayor de San Marcos [5].

La solución de voto electrónico presencial en el Perú, consta como mínimo de 2 equipos para dar servicio a una mesa de votación conformada por aproximadamente 600 electores. Los dos equipos tienen las mismas características físicas pero en la mesa de votación tienen diferentes funciones. Los equipos no tienen ninguna conexión física entre ellos; un equipo permite la identificación del elector a través de la lectura del número de su DNI mediante un escáner, o digitando en la pantalla táctil los números del DNI, luego de comprobar que el elector pertenece a la mesa de votación, se activa una tarjeta inteligente habilitadora, la cual le permitirá realizar un solo voto en el otro equipo denominado cabina de votación. En la cabina de votación, el elector introduce la tarjeta inteligente activa, en la ranura del lector de tarjetas; la aplicación de voto electrónico le presenta la cédula de votación para que pueda ejecutar un solo voto. El elector selecciona la agrupación política, el candidato de su preferencia o voto en blanco, luego corrige o confirma su elección, al confirmar se imprime en papel térmico un comprobante el cual muestra la elección del elector, terminando el proceso para el elector.

Los equipos de voto electrónico de la ONPE se utilizaron en el proceso electoral de Segunda Elección Presidencial 2011, en el distrito de Pacarán, Provincia de Cañete, departamento de Lima [6].

Los componentes del equipo de voto electrónico presencial peruano son:

- Una computadora de tipo industrial de bajo consumo
- Baterías de tipo ácido-plomo
- Monitor LCD
- Una tarjeta de control de datos y del sistema de energía
- Un lector de códigos de barras
- Un lector de tarjetas inteligentes
- Una impresora térmica
- Una lámina táctil
- Chasis de fibra de vidrio
- Tres compuertas para conexión de dispositivos (dos controladas electrónicamente)

La aplicación de voto electrónico está desarrollada en el lenguaje de programación C++, sobre el sistema operativo Linux. En la figura N° 1.3 se muestra el equipo de voto electrónico utilizado actualmente en el Perú.



Figura 1.3 Equipo de voto electrónico utilizado en el Perú

### 1.6 Propuesta de equipo de voto electrónico presencial

El presente trabajo, propone un equipo de votación con la función de cabina de votación, reduciendo el consumo de energía eléctrica y manteniendo el requisito del tiempo de autonomía eléctrica para funcionar toda la jornada electoral. Para minimizar el consumo de energía en comparación con el equipo de voto electrónico presencial peruano, se descartó el uso del monitor LCD y la impresora de papel térmico. Se descartó el uso de una computadora debido a que este componente está sobredimensionado para la aplicación, dado que la función principal es el conteo de votos y esto se puede realizar con un computador con menos prestaciones. El equipo de Voto Electrónico Presencial (VEP) propuesto elimina la impresión del voto dado que no se utilizarán las impresiones para obtener los resultados electorales. La consolidación de resultados se realiza en una computadora personal, en el cual se imprimen los resultados de la mesa de votación. El equipo de voto electrónico presencial propuesto permite al elector ejercer su derecho de elegir. El equipo permite la selección de un candidato, de la cédula de votación impresa en papel. El dispositivo de entrada de datos es una lámina sensible al tacto que permite seleccionar un candidato de la lista, esta selección ocurre al observar la luz de color rojo de un diodo emisor de luz, al costado de la imagen del símbolo de la agrupación política. El equipo es habilitado para permitir la ejecución de un solo acto de votación, realizado por un elector, mediante una llave electrónica conectada al equipo. En la conexión de la llave se implementa un canal de comunicación con un protocolo serial. Los resultados de la votación son almacenados en la llave electrónica y presentados al final de la jornada de votación mediante una aplicación de software mostrada en una computadora personal.

## 1.7 Objetivos

### Principal

Diseño e implementación de un equipo de voto electrónico con la función de cabina de votación, el cual muestra la lista de candidatos impresa en papel, detrás de una lámina táctil. Se utiliza una llave de activación para habilitar el equipo y realizar un voto por elector.

### Específicos

- Procesar la información de las coordenadas que entrega la lámina táctil al ser presionada en un punto.
- Almacenar la información de las coordenadas de los puntos que conforman la cédula de votación.
- Establecer una comunicación serial half dúplex, a través de un pin entre el microcontrolador principal y el microcontrolador de la llave de activación.
- Activar la cabina de votación al reconocer la información entregada por la llave de activación.
- Mostrar la selección de un candidato a través de diodos emisores de luz.
- Almacenar la información de los resultados electorales en una memoria no volátil.

## 2 DISEÑO E IMPLEMENTACIÓN DEL HARDWARE

### 2.1 Principales requerimientos

Actualmente en un proceso electoral se utilizan cédulas de votación, es decir, papel impreso con las opciones de los candidatos, en las cuales se realizan marcas con lapicero para manifestar la preferencia del elector. Para mantener la similitud del procedimiento manual con el electrónico, se utiliza una cédula impresa en papel, manteniendo el símbolo y rostro de los candidatos en la cédula.

Los principales requerimientos que el equipo de voto electrónico debe cumplir para una producción en serie son:

- **Bajo costo.**  
Basado en circuitos electrónicos de aplicación específica.
- **Energía eléctrica proveída por baterías.**  
Permite que el equipo sea portátil.
- **Tiempo de autonomía de energía eléctrica mayor a 12 horas.**  
El proceso electoral comienza a las 08:00 horas y culmina a las 16:00 horas, necesitándose además tiempo para la instalación de la mesa de votación, tiempo para el cierre de la jornada electoral y tiempo de respaldo ante una evento imprevisto.
- **Presentación de la cédula de votación y registro de votos.**  
Mantiene la similitud con el proceso de votación manual, al mostrar la cédula electoral, permitiendo que la transición al nuevo sistema sea simple.
- **Habilitación para la ejecución de un voto por elector.**
- **Portátil, de bajo peso y volumen.**  
Reduce los procesos y costos logísticos.
- **Seguro**  
Protege la información y permite su auditoría.
- **Componentes electrónicos vigentes en el mercado durante un gran periodo de tiempo.**

Para evitar el desabastecimiento de componentes electrónicos y lograr el retorno de inversión de la aplicación de voto electrónico por el sistema manual.

## 2.2 Componentes de la solución

El diagrama de bloques propuesto se muestra en la figura N° 2.1, el cual está compuesto por:

### Lámina táctil

A través de la presión con el dedo sobre ella, permite que el elector seleccione la agrupación política de su preferencia. El papel impreso con la cédula de votación se coloca debajo de la lámina táctil; muestra los símbolos y nombres de las agrupaciones políticas. La información de las coordenadas del punto de presión es enviada al puerto UART del microcontrolador.

### Microcontrolador A

- Procesa la información de las coordenadas de los puntos de presión sobre la lámina táctil.
- Monitorea el valor del voltaje de las baterías para determinar la autonomía de energía eléctrica que tiene el equipo.
- Se comunica a través de un pin con el microcontrolador B para leer el estado (habilitado o deshabilitado) de la llave de habilitación de equipo.

### Dispositivo Visual

Se utilizan diodos emisores de luz, los cuales cumplen las siguientes funciones:

- Le indican al elector que el equipo está habilitado o no, para poder ejecutar un solo voto.
- Le muestran al elector su elección por una agrupación política al tocar la lámina táctil en la imagen mostrada en la cedula de votación impresa en papel, la cual está colocada debajo de la lámina táctil.
- Le indican al elector que puede cambiar su elección o confirmarla.

### Generador de Sonido

Genera sonidos que permiten reconocer un proceso asociado.

El sonido generado al tocar la lámina táctil, le ayuda al elector en el proceso de votación.

**Microcontrolador B**

Se comunica a través de un pin con el microcontrolador A para entregar el estado (habilitado o deshabilitado) de la llave de habilitación de equipo.

Se comunica con la computadora personal para adquirir el estado habilitado de la llave de habilitación de equipo y para entregar la información de los votos por agrupación política almacenados en su memoria EEPROM.

**Computadora Personal**

Permite a través de una interface de software habilitar la llave de habilitación y mostrar los resultados electorales.

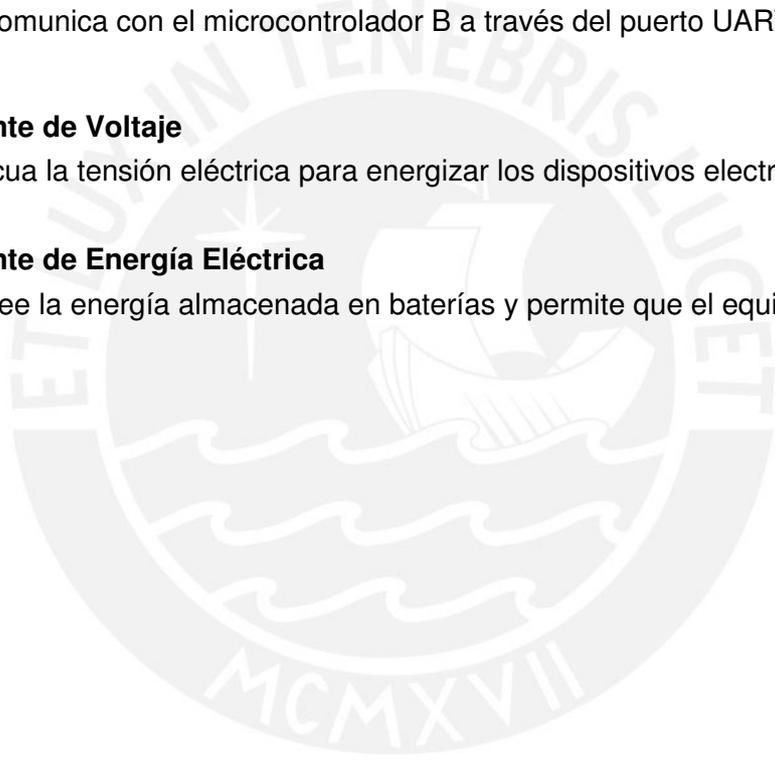
Se comunica con el microcontrolador B a través del puerto UART.

**Fuente de Voltaje**

Adecua la tensión eléctrica para energizar los dispositivos electrónicos.

**Fuente de Energía Eléctrica**

Provee la energía almacenada en baterías y permite que el equipo sea portátil.



### Diagrama de Bloques del Equipo de Voto Electrónico

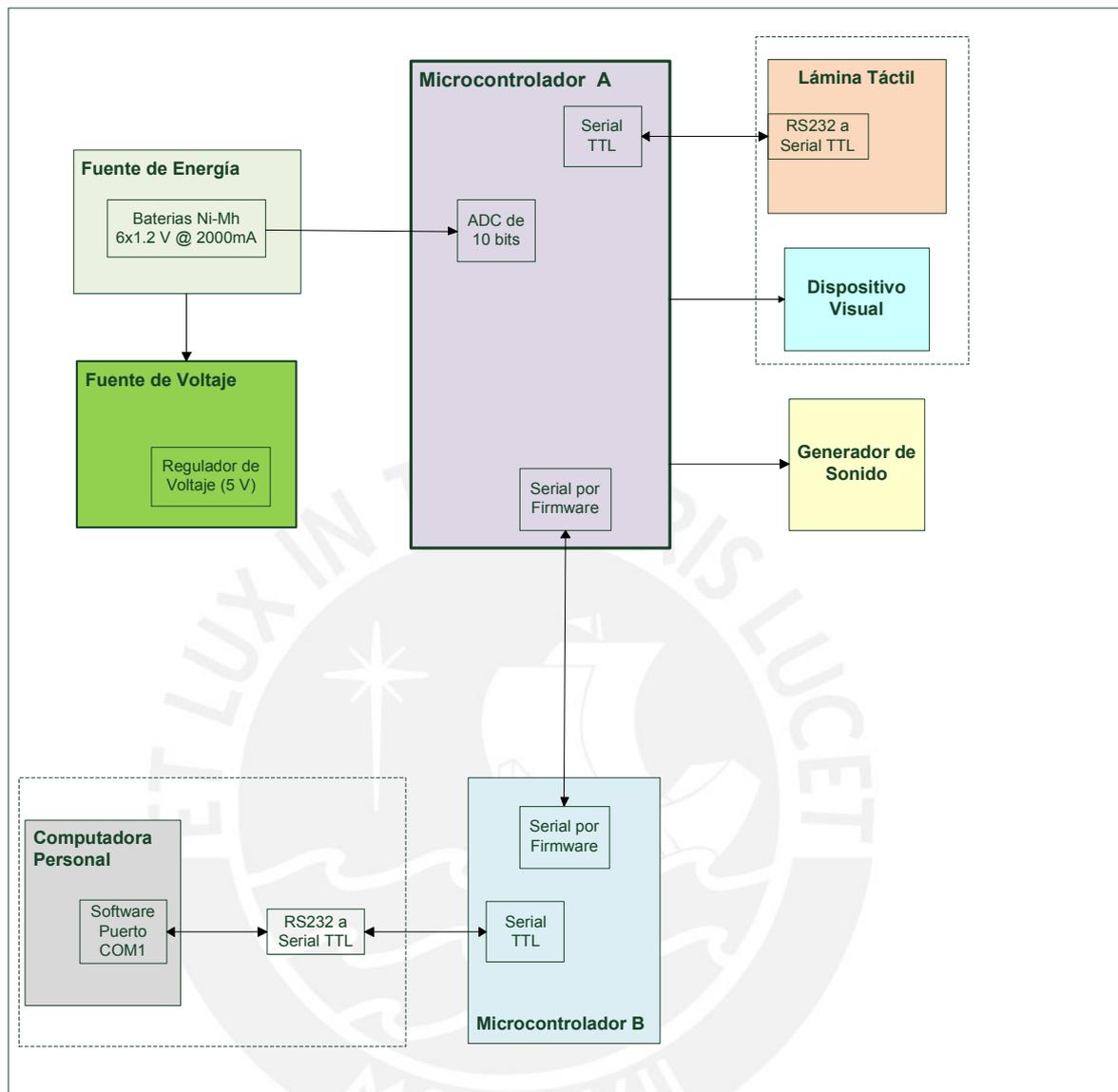


Figura 2.1

A continuación se desarrolla cada uno de los bloques:

#### 2.2.1 Lámina Táctil

Para mantener una similitud con el equipo de voto electrónico peruano se optó por utilizar una lámina táctil como dispositivo de entrada de datos. Entre las tecnologías disponibles tenemos:

- Resistiva
- Superficie Capacitiva
- Onda de Superficie acústica
- Infrarrojo

Tabla 2.1. Características de la lámina táctil de acuerdo a su tecnología [7], [8].

Especificación	Resistiva de 5 cables	Superficie capacitiva	Onda de Superficie acústica	Infra-Rojo
Precisión	0.080"	1.50%	<± 1% X & Y	± 0.125"
Toque con guantes	todo tipo	no	todo tipo	todo tipo
fuerza de activación	de 115 g hasta 350 g	50 g	85 g	No requiere
estabilidad de la calibración	buena	muy buena	auto calibración	muy buena
claridad óptica	hasta 80%	hasta 85%	92%	100%
Resistencia a la luz intensa	buena	mala	buena	mala
durabilidad	5 años	2 años	5 años	5 años
costo	Bajo (tamaños pequeños)	moderado	alto	alto

Elaboración: [7], [8].

De la tabla 2.1 se observa que la lámina táctil de tecnología resistiva tiene un costo menor, una precisión aceptable y se presiona con o sin guantes, por lo que se elige este tipo de lámina. [7]. [8]. Se utiliza una lámina táctil con las dimensiones 41 cm x 25.6 cm, de tecnología resistiva de 5 hilos. Los datos de las coordenadas son adquiridos por el microcontrolador a través de una comunicación serial RS232 con el controlador de la lámina táctil. La cédula de votación impresa en papel, se coloca debajo de la lámina táctil para indicarle al elector en que zonas debe tocar la lámina.

### Coordenadas del punto de presión

La información que entrega el controlador de la lámina táctil está adecuada para ser obtenida a través de un puerto serie de una computadora con un conector DB9 macho. En la tarjeta controladora se utiliza el circuito integrado MAX232 con un conector DB9 macho, para adaptar las señales con el protocolo RS232 a señales TTL del microcontrolador. Este circuito integrado utiliza 5 condensadores de 100 nF, de acuerdo a la especificación de su hoja técnica [12].

La configuración de la comunicación serial del controlador de la lámina táctil es 9600 bps, 8 bits de datos, sin paridad y un bit stop. Esta velocidad de transmisión es fija para el controlador de la lámina táctil por lo que se configura la velocidad de comunicación serial del microcontrolador a este valor.

Según la hoja técnica del controlador de la lámina táctil, los datos de la posición de un punto bajo presión son transmitidos en 5 bytes continuamente hasta que se libere la presión.

El primer byte indica que existe presión en la lámina: 81 h

El segundo y tercer byte indican la coordenada x: XX XX h

El cuarto y quinto byte indican la coordenada y: YY YY h

Cuando se libera la presión se transmite un solo byte: 80h

Se toma como el origen de coordenadas, el vértice superior izquierdo del rectángulo, cuando el conector de 5 hilos se encuentra en la parte inferior derecha (Figura 2.2). La posición permite utilizar la lámina con la menor dimensión como eje x y la mayor dimensión como el eje y.



Figura 2.2 Lámina táctil

El controlador de la lámina táctil se energiza con 5V y la corriente de consumo es de 21 mA, cuando no hay presión sobre la lámina. Cuando hay presión sobre un punto de la lámina, la corriente se incrementa hasta 71 mA.

## 2.2.2 Microcontrolador A

### Requerimientos del Microcontrolador

Para realizar el procesamiento de la información se seleccionará un microcontrolador que permita:

- Controlar la información entregada por la lámina táctil a través de una comunicación serial.
- Gestionar la comunicación con la llave habilitadora a través de un protocolo serial implementado sobre un pin de entrada / salida del microcontrolador.
- Gestionar la señalización de 16 diodos emisores de luz, para indicar la selección del candidato realizada por el elector.
- Gestionar la señalización de 4 diodos emisores de luz, para indicarle al elector los pasos seguidos al votar.
- Gestionar la señalización de 3 diodos emisores de luz, para indicar el nivel de energía de las baterías.
- Gestionar la señalización sonora.
- Almacenar la información del registro de votos.

### Selección del microcontrolador

La información que entrega el controlador de la lámina táctil se obtiene a través de una comunicación serial a 9600 bps, 8 bits de datos, sin paridad y un bit de parada.

El microcontrolador debe tener un puerto UART para obtener los datos de los toques sobre la lámina. Las consideraciones para seleccionar un microcontrolador en relación al número de pines de entrada / salida son:

- Para la comunicación serial asíncrona con el controlador de la lámina táctil, se requiere un puerto UART, es decir, dos pines de entrada / salida.
- Para la comunicación con la llave habilitadora, se necesita un pin de entrada / salida del micro controlador, para implementar una comunicación half dúplex sobre un pin de entrada / salida.
- Para mostrar la elección de un candidato de la cédula de votación, se necesitan 5 pines de salida para controlar un decodificador de 4:16 y un habilitador del chip.
- Para la señalización del proceso de votación se necesitan 4 pines de salida, para indicar los estados: activo, desactivo, corregir, confirmar.
- Para mostrar el nivel de energía eléctrica que puede proveer la batería, se necesitan 3 pines de salida y un pin de entrada para el ADC.

- Para generar sonidos de alerta a través de un zumbador (buzzer), se necesita un pin de salida.
- Para tomar las muestras del voltaje de la batería se necesita un pin de entrada.

En la tabla N° 2.2 se muestra el resumen de los pines de entrada / salida necesarios para implementar las funciones del equipo

Tabla 2.2. Uso de los pines del microcontrolador.

Funciones del equipo	pines necesarios
Puerto UART	2
Implementación de UART por software	1
Visualización de elección - Decodificador 4:16 - Habilitador	5
Señalización de votación ( 4 LED )	4
Mostrar el nivel de energía eléctrica ( 3 LED )	3
Muestras del voltaje de la batería	1
Generar sonidos	1
	<b>17</b>

Elaboración: propia.

En total se necesitan 17 pines de entrada / salida. El equipo puede atender en una jornada electoral de 8 horas a 600 electores aproximadamente, con lo cual cada agrupación política puede obtener esta cantidad de votos como máximo. Para almacenar este número se necesitan 10 bits, pero en forma práctica se utilizan 2 bytes. El número de opciones en la cédula de votación es de 15 agrupaciones políticas y una opción "VOTO EN BLANCO", con lo cual se necesitan  $16 \times 2 = 32$  bytes de memoria EEPROM. No se tiene como opción el voto nulo o viciado.

Cada punto de la lámina táctil tiene una posición (x,y), y esta posición es almacenada en 4 bytes. Para configurar la cédula de votación se construyen rectángulos los cuales representan las áreas o botones a presionar, por lo que se requieren 2 puntos para construir un botón y entonces se necesitan 8 bytes de memoria para almacenar las coordenadas de los 2 puntos del rectángulo que define el botón. Se implementan 16 botones de opciones y dos botones de control (CONFIRMAR y CORREGIR), con lo cual se necesitan  $18 \times 8 = 144$  bytes de memoria EEPROM. En total se necesitan por lo menos:

$$16 \times 2 \text{ bytes} + 18 \times 8 \text{ bytes} = 176 \text{ bytes de memoria EEPROM}$$

En el mercado local se disponen de las siguientes opciones (Tabla 2.3) que cumplen los requerimientos:

Tabla 2.3. Microcontroladores en el mercado local

MCU Modelo	Marca	pinos de E/S	USART	canales ADC	Contadores	Memoria de Programa	Memoria RAM	Memoria EEPROM	Proveedor local	Costo(S./.)
ATmega88PA	Atmel	23	1	6 / 8 (10b)	2 de 8 y 1 de 16 bits	8KB	1KB	512 bytes	DIAC	13.5
PIC16F876A-I/PA	Microchip	22	1	5 (10b)	2 de 8 y 1 de 16 bits	14K B	368 bytes	256 bytes	HI FI	17.2

Elaboración: propia.

Se seleccionó el microcontrolador modelo ATmega88 de la marca ATMEL [20], que además de cumplir los requerimientos tiene un menor costo.

### Convertor Análogo Digital

Para conocer cuánto tiempo de autonomía de energía eléctrica tiene el equipo para seguir operando, se utiliza un Convertor Análogo Digital con la finalidad de obtener el valor de voltaje que tiene el arreglo de pilas. Con el valor del voltaje, la corriente de descarga y las gráficas proporcionadas por el fabricante de las baterías, se puede aproximar el tiempo de autonomía del equipo y cuanto de tiempo le queda por operar en un determinado momento.

El rango de voltaje del conjunto de 6 baterías AA es  $6 \times [1.1, 1.4]$  Voltios =  $[6.6, 8.4]$  Voltios, donde 6.6 voltios indica que el conjunto de baterías está descargado y 8.4 Voltios indica 100% de carga. El voltaje en el diodo es 0.7V por lo que la diferencia de voltaje estará en el rango de  $[5.9, 7.7]$  V. Para adecuar el voltaje de las baterías al rango de  $[0V, 5V]$ , dado por el voltaje de referencia  $V_{ref}=5$  V del microcontrolador, se usan dos resistencias, teniendo en cuenta que la corriente de fuga de 1uA en el pin de entrada del ADC, no varíe significativamente el voltaje que será muestreado (Figura 2.3). El voltaje presente en el pin de entrada del ADC es igual a:

$$V_{adc} = \frac{4.7K\Omega}{4.7K\Omega + 3.3K\Omega} * [5.9V, 7.7V] = [3.46V, 4.52V]$$

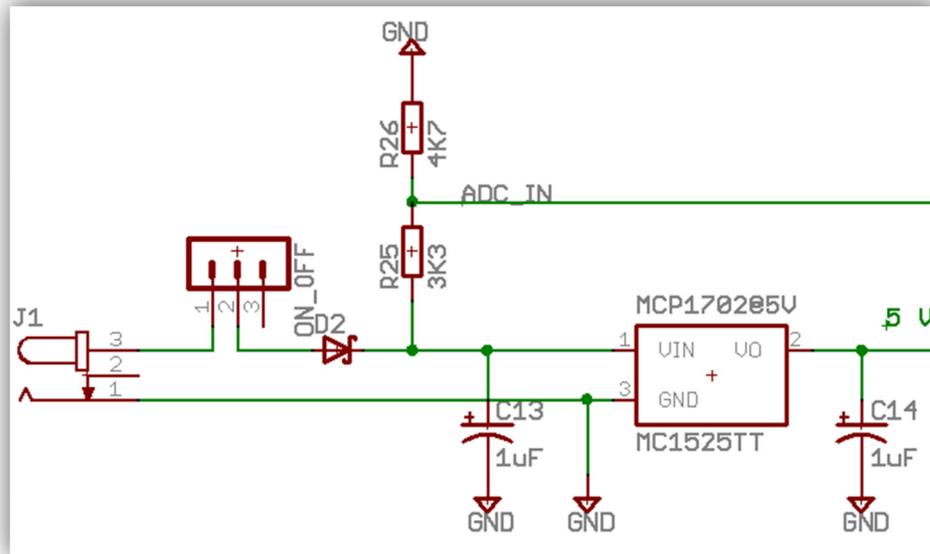


Figura 2.3 Voltaje de entrada al ADC

La resolución del ADC es de 10 bits y el voltaje de referencia del ADC es  $V_{ref} = 5\text{ V}$ .

- El valor de voltaje de 4.52 V indica que las pilas tienen 100% de carga y su valor en código binario obtenido por el ADC es 39Dh
- El valor de voltaje de 3.46 V indica que las pilas están descargadas y su valor en código binario obtenido por el ADC es 2C4h

El valor obtenido por el ADC se utiliza para clasificar y mostrar el tiempo de autonomía, encendiendo un solo LED con la finalidad de ahorrar energía y de acuerdo a los siguientes rangos:

- LED de color verde encendido:  
14 h < tiempo de autonomía < 40 h, Rango de voltaje: [4.01 V, 4.52 V]
- LED de color ámbar encendido:  
2 h < tiempo de autonomía < 14 h, Rango de voltaje: [3.65 V, 4.00 V]
- LED de color rojo encendido:  
0 h < tiempo de autonomía < 2 h, Rango de voltaje: [3.46 V, 3.64 V]

### 2.2.3 Dispositivo Visual

Debido al requerimiento de menor consumo de energía eléctrica por ser un equipo portátil energizado con baterías, se tiene como opciones:

- Arreglos de diodos emisores de luz (display de segmentos).
- diodos emisores de luz.

Se eligió utilizar diodos emisores de luz por tener bajo consumo de energía eléctrica y ocupar un menor espacio en el equipo.

Para poder indicarle al elector en que parte del proceso de votación se encuentra, se utilizan 4 diodos emisores de luz. Las asociaciones entre las luces de los diodos y los mensajes son:

- Diodo de color verde encendido, ubicado en la parte superior derecha, indica que el equipo se encuentra habilitado para votar.
- Diodo de color rojo encendido, ubicado en la parte superior izquierda, indica que el equipo se encuentra deshabilitado para votar.
- Diodo de color verde encendido, ubicado en la parte inferior derecha, indica que el elector debe confirmar su elección, con lo cual termina el proceso de votación.
- Diodo de color rojo encendido, ubicado en la parte inferior central, indica que el elector puede cambiar su elección.

Si la llave habilitadora (plug de audio) está activa cuando se introduce en el jack de audio entonces se habilita el equipo para poder votar, esto es indicado mediante la luz de un LED (SEÑALIZACION\_0) de color verde. Si la llave habilitadora no está activa al introducirla en el equipo, se indica mediante la luz de un diodo LED (SEÑALIZACION\_1) de color rojo.

El microcontrolador A utiliza un circuito integrado decodificador 74HC154 de 4:16 conectado a 16 LEDS en serie con resistencias de 330 Ohmios. Con 4 bits se selecciona el diodo que se iluminará, indicándole al usuario cual fue la agrupación política que eligió en una cedula de tipo cerrada, es decir, solo se puede votar por un candidato. Se pueden seleccionar uno de 15 candidatos o seleccionar VOTO EN BLANCO.

Un LED (SEÑALIZACION\_3) indica si se desea corregir la selección del candidato y otro LED (SEÑALIZACION\_4) indica que se debe confirmar el voto para terminar el proceso.

El equipo de voto electrónico no imprime el comprobante de voto debido a que no se utilizan las impresiones para realizar el conteo de votos, ya que este proceso es automático y es una de las virtudes del voto electrónico.

#### **2.2.4 Generador de Sonido**

Las señales audibles nos permiten reconocer fácilmente ciertos eventos programados sin necesidad de trabajar directamente con el equipo para saber su estado. Se generan señales audibles con la finalidad de ayudar al elector en el proceso de votación y también facilitar el proceso de capacitación.

Se utiliza un zumbador que funciona a 5V, con una corriente de consumo de 35.2 mA, a una frecuencia de 3950 Hz con una onda cuadrada generada por el microcontrolador. La corriente máxima del zumbador es de 50mA y tiene una resistencia de 38 Ω.

La señal cuadrada generada es de 50% de ciclo de trabajo, la cual excita la puerta de un transistor MOSFET RK7002B [21], logrando que trabaje en conmutación. El voltaje de umbral para la conducción es  $V_{gs}(Th)=2.3$  V. La resistencia de 100Ω en serie con el zumbador, permite que el valor de la corriente que pasa por el zumbador esté en su rango de operación. La figura 2.4 muestra el circuito implementado para generar el sonido.

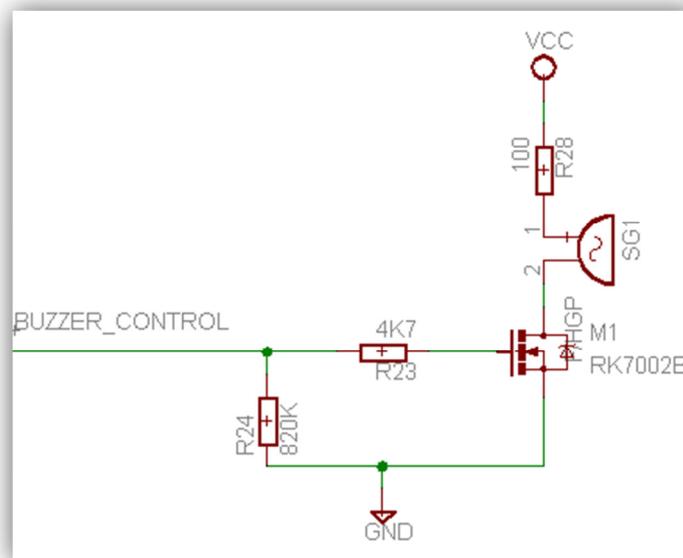


Figura 2.4 Generación del sonido

Análisis del MOSFET en conmutación:

MOSFET canal N en Corte:

$$V_{control}=0 \text{ V} \longrightarrow V_{gs} = 0 < V_{gs}(Th)=2.3\text{V} \longrightarrow I_{ds}=0 \text{ A}$$

MOSFET canal N Activo:

$$V_{cc}=5 \text{ V} , R_{buzzer}= 38 \Omega , R_{28}=100\Omega$$

$$V_{control}=5 \text{ V} > V_{gs}(Th)=2.3\text{V} \longrightarrow \text{Si } V_{gs}=5 \text{ V de las hojas de datos del MOSFET se obtiene: } R_{ds}(ON)= 2 \Omega , I_{ds}/V_{ds}=0.5 \text{ A/V} \dots (1)$$

$$\text{Entonces } I_{ds} = (5\text{V}-V_{ds}) / (100\Omega+38\Omega+2\Omega) = 35.2 \text{ mA}$$

$$I_{ds} = (5V - 2 \cdot I_{ds}) / (100\Omega + 38\Omega + 2\Omega) = 35.2 \text{ mA}$$

De (1):

$$V_{ds} = I_{ds}(2 \Omega) = 70.4 \text{ mV.}$$

$$\longrightarrow V_{ds} < V_{gs} - V_{Th}$$

$$0.0704V < 5V - 2.3V$$

Se verifica que el MOSFET de canal n se encuentra en la Región Óhmica.

## 2.2.5 Microcontrolador B

### Requerimientos del Microcontrolador

Para realizar el procesamiento de la información se seleccionará un microcontrolador que permita:

- Controlar la información entregada por la computadora personal a través de una comunicación serial asíncrona.
- Almacenar la información de los resultados electorales por agrupación política.
- Gestionar la comunicación con la tarjeta controladora a través de un protocolo serial implementado sobre un pin de entrada / salida del microcontrolador.
- Habilitar la cabina de votación para que el elector vote una sola vez.

### Selección del microcontrolador

Para simplificar el diseño y desarrollo del equipo, se utiliza el mismo modelo de microcontrolador seleccionado anteriormente (ATMEGA 88), dado que tiene un bajo costo y se puede reutilizar el código fuente del firmware para la comunicación sobre un pin, disminuyendo el tiempo de implementación.

## 2.2.6 Computadora Personal

Permite a través de una interface de software:

- Habilitar la tarjeta Llave de habilitación, la cual habilita al equipo para poder votar.
- Mostrar al final de la jornada electoral los resultados electorales.

El desarrollo de la aplicación se muestra en el capítulo N° 4 Implementación del software.

## 2.2.7 Fuente de Voltaje

Los circuitos integrados que se seleccionaron se energizan con 5V DC. Para conseguir este voltaje a través de baterías, se seleccionó el regulador de voltaje MCP-1702@5V de

la marca Microchip [9] por tener un bajo costo, bajo voltaje de caída de entrada-salida, entrega hasta 250mA y ocupa un menor espacio en la tarjeta por tener un empaque superficial.

Las hojas técnicas del regulador MCP-1702@5V especifican lo siguiente:

- La caída máxima de voltaje en el regulador es 0.650 V a la corriente de carga de 250mA y  $V_r = 5$  V.
- El voltaje de salida regulado es:  $[V_r - 3\%V_r, V_r + 3\%V_r]$

Por lo que el voltaje en la entrada del regulador debe ser mayor a  $(V_r + 0.03 * V_r + 0.650V) = 5.8$  V, donde  $V_r$  es el Voltaje de regulación y es igual a 5V.

Para obtener el voltaje regulado de 5 V se necesita un voltaje de entrada mayor a 5.8 Voltios y menor a 13.2V en la entrada del regulador, de acuerdo a las especificaciones del fabricante, mostradas en la hoja técnica.

### 2.2.8 Fuente de Energía Eléctrica

Para que el equipo sea portátil debe energizarse con baterías. Las baterías que se seleccionen deben contribuir con las características del equipo, entre las cuales está el bajo peso, el menor volumen y el mayor tiempo de autonomía eléctrica.

En la tabla 2.4 se muestran las características por tipo de batería [26].

Tabla 2.4 Comparación entre tipos de baterías

	Ni-MH	Lead Acid	Li-ion	Li-ion polymer
Densidad de energía gravimétrica (Wh/kg)	60-120	30-50	110-160	100-130
Costo de batería típica (US\$, referencial)	\$60 (7.2V)	\$25 (6V)	\$100 (7.2V)	\$100 (7.2V)
Voltaje de celda (nominal)	1.25V	2V	3.6V	3.6V
Tiempo de carga rápida	2-4h	8-16h	2-4h	2-4h
Auto descarga / mes	30%	5%	10%	~10%
Ciclo de vida (a 80% de capacidad inicial)	300 a 500	200 a 300	500 a 1000	300 a 500
Corriente de carga (A)				
- Pico	5C/1h	5C/1h	>2C/1h	>2C/1h
- mejor resultado	0.5C/1h o menor	0.2C/1h	1C/1h o menor	1C/1h o menor
Mantenimiento requerido	60 a 90 días	3 a 6 meses	No requiere	No requiere
Costo por ciclo(US\$)	\$0.12	\$0.10	\$0.14	\$0.29

Elaboración: [26]

La tasa C indica la capacidad de corriente de carga y descarga de una batería, expresada en Ah.

1C, significa que una batería de 1000 mAh que se descarga a la tasa de 1C en condiciones ideales debería proporcionar una corriente de 1000 mA durante una hora. La misma batería que se descarga a 0,5 C proporcionaría 500 mA durante dos horas, y a 2C, la batería de 1000 mAh entregaría 2000 mA durante 30 minutos. 1C es también conocida como una descarga de una hora, un 0.5 C es una descarga de dos horas, y un 2C es una descarga media hora.

Para la selección de las baterías, se tomó en cuenta lo siguiente:

- capacidad de entregar corriente
- costo
- peso
- volumen

Las baterías recargables tipo Ni-MH en el formato AA conocidas como pilas recargables son muy populares en el mercado local y son utilizadas principalmente para energizar juguetes.

Se seleccionó el tipo de baterías recargables Ni-MH (Nickel-metal-hydride) en formato AA por tener gran capacidad de energía acumulada, bajo peso y bajo costo por ciclo.

El formato AA de las baterías es muy utilizado en el mercado local.

### **Tiempo de autonomía de energía eléctrica**

Para determinar el tiempo de autonomía de energía eléctrica del equipo, se necesita conocer la energía eléctrica que consume cada componente del equipo y la energía que pueden proveer las baterías.

El circuito de alimentación posee un diodo de protección de polaridad inversa, el cual al conducir presenta en sus terminales 0.7 V, por lo que a la entrada del regulador, el voltaje es igual al voltaje del arreglo de pilas menos el voltaje en el diodo. El conjunto de pilas debe entregar un voltaje mayor a  $6.5 \text{ V} = 5.8 \text{ V} + 0.7 \text{ V}$ , por lo tanto se necesitan 6 pilas recargables de 1.2 Voltios colocadas en serie, para alimentar el circuito.

En el acto de votación el consumo máximo ocurrirá cuando la lámina táctil es presionada, se tienen encendidos 5 diodos emisores de luz (habilitado, candidato seleccionado, corregir, confirmar y un diodo que indican el nivel de voltaje) y está conectada la llave de habilitación.

En la tabla 2.5 se muestran los consumos de energía aproximados para los componentes del equipo de voto electrónico.

Tabla 2.5 Consumo eléctrico de los componentes del equipo

Componentes principales	cantidad	voltaje (V)	corriente (mA)	potencia (mW)	fracción de uso en una hora	(mA-h)	energía (mW-h)
Tarjeta controladora	1	5	16	80	1	16	80
Lámina táctil (stand by)	1	5	21	105	1	21	105
Llave habilitadora (circuito)	1	5	9	45	0.625	5.625	28.125
lámina táctil (ON)	1	5	50	250	0.083	4.166	20.833
Zumbador	1	5	35.2	176	0.083	2.9216	14.608
Conjunto de LED activos	1	5	9.875	49.375	1	9.875	49.375
						59.588	297.941

Elaboración: propia

En el mercado local se consiguieron pilas AA recargables de marca GP modelo GP210AAHC las cuales tienen una capacidad de 2000 mAh. De la curva de descarga a 10% de su capacidad (200mA), se obtiene que el voltaje de la pila cuando esta descargada es aproximadamente de 1.1 V y cuando está totalmente cargada su voltaje es 1.4 V [10]. Asumiendo el peor caso, cuando están descargadas, el voltaje del conjunto de 6 pilas será de  $1.1 \text{ V} \times 6 = 6.6 \text{ V}$ . y cuando estén con una carga de 100% el voltaje del arreglo será de  $6 \times 1.4 \text{ V} = 8.4 \text{ V}$ .

La energía que puede proveer el conjunto de 6 pilas AA es:

$$14400 \text{ mW-h} = 6 \times 1.2 \text{ V} \times 2000 \text{ mA-h}$$

La corriente de carga (promedio) es  $I_L = 59.58 \text{ mA}$

La potencia eléctrica de la carga es:

$$5 \text{ V} \times I_L = 5 \text{ V} \times 59.58 \text{ mA} = 297.9 \text{ mW}$$

Según las hojas de datos del fabricante del regulador, la potencia eléctrica disipada por el regulador es:

$$(7.2 \text{ V} - 5 \text{ V}) \times I_L = 2.2 \text{ V} \times 59.58 \text{ mA} = 131.07 \text{ mW}$$

La potencia eléctrica total consumida es:  $297.9 \text{ mW} + 131.07 \text{ mW} = 428.97 \text{ mW}$

El tiempo de autonomía eléctrica del equipo es:

$$14400 \text{ mW-h} / 428.97 \text{ mW} = \boxed{33.56 \text{ horas}} \text{ aproximadamente.}$$

### 2.3 Tarjeta Controladora

Se diseñaron dos tarjetas electrónicas, una de ellas denominada Tarjeta Controladora y la otra denominada Tarjeta Llave de habilitación. Ambas tarjetas se construyeron con componentes electrónicos superficiales con la finalidad de reducir al máximo el espacio ocupado.

Las dos tarjetas utilizan el mismo modelo de microcontrolador de la marca Atmel modelo ATmega88PA y se energizan con 5 V DC. Entrega hasta 250mA de corriente, suficientes para la aplicación, dado que el consumo de todos los dispositivos incluyendo la llave de habilitación, en el peor caso es de 149mA. El regulador de voltaje MCP-1702@5V utiliza un condensador de entrada de 1uF y un condensador de salida de 1 uF [9].

Se seleccionó un cristal de 4 Mhz de bajo costo (SIWARD 6F), debido a que la frecuencia del oscilador interno varía con la temperatura, se requiere tener una base de tiempo estable y se disminuya el consumo de energía del microcontrolador, que depende también de la frecuencia de oscilación del cristal.

Se utiliza un diodo de protección contra el voltaje inverso, en la entrada del regulador de 5 V.

El diodo seleccionado es M7 (SMD-4007) de empaque superficial,  $V_d=0.7$  V y soporta hasta 1 A de corriente, suficiente para soportar la corriente máxima de todos los componentes de la tarjeta.

Se utilizan una resistencia de 10 K $\Omega$  en pull-up en el pin RESET del microcontrolador, 2 capacitores de 22 pF en el circuito del cristal, un condensador de desacoplo de 100 nF entre VCC y GND, un condensador de desacoplo de 100 nF entre AVCC y GND, y un condensador de desacoplo de 100 nF entre AREF y GND. Estos valores se obtuvieron de las recomendaciones del fabricante de microcontroladores [11]. En la figura 2.5 se muestra el diagrama esquemático de la Tarjeta Controladora.



Figura 2.5 Diagrama esquemático de la Tarjeta Controladora

## 2.4 Tarjeta Llave de Habilitación

La Tarjeta Llave de habilitación permite activar el equipo de voto electrónico para que el elector vote una sola vez. La activación de la llave se realiza en una computadora personal a través del puerto serial y gobernada por una aplicación en software desarrollada para este fin. La llave habilitadora graba la información de los votos en una memoria EEPROM y los resultados electorales se presentan después de cerrar la mesa de votación mediante la aplicación de software.

El hardware de la llave habilitadora utiliza un micro controlador ATmega88, un chip MAX232 para conectar la llave al puerto serie de la computadora personal y un conector de audio macho de 3 líneas. El conector de audio se eligió con la finalidad que el elector introduzca la llave en el equipo de voto, sin preocuparse del sentido en el cual se coloca la llave, ya que es circular. Este conector es muy común en el uso de equipos de audio por lo que le es muy familiar al elector (Figura 2.6).

Se diseñó la tarjeta electrónica para que ocupe un pequeño espacio, con la finalidad de acoplarla al conector de audio. Para el diseño se consideró usar componentes superficiales con la finalidad de minimizar el tamaño de la tarjeta. En la figura 2.7 se muestra el diagrama esquemático de la Llave de habilitación.



Figura 2.6 Empaque del circuito de habilitación (llave de habilitación)



Figura 2.7 Diagrama esquemático de la Llave de habilitación

### 3 DISEÑO E IMPLEMENTACIÓN DEL FIRMWARE

Para controlar el hardware del equipo de voto electrónico, se programó el firmware del microcontrolador de la tarjeta Controladora en lenguaje ensamblador, las funciones programadas son las siguientes:

- Obtención de las coordenadas (x, y)
- Configuración de la cédula de votación
- Señalización de diodos emisores de luz (LED) al votar
- Comunicación equipo – llave
- Protocolo de comunicación sobre un cable

Se programó el firmware del microcontrolador de la tarjeta Llave de Habilitación, con las siguientes funciones:

- Protocolo de comunicación equipo – llave
- Protocolo de comunicación sobre un pin.

#### 3.1 Obtención de las coordenadas (x, y)

Permite obtener las coordenadas del punto de presión de la lámina táctil, de un conjunto de coordenadas entregadas por el controlador de la lámina táctil. En el Diagrama N° 3.1 se muestra el diagrama de flujo de adquisición de datos de la lámina táctil.

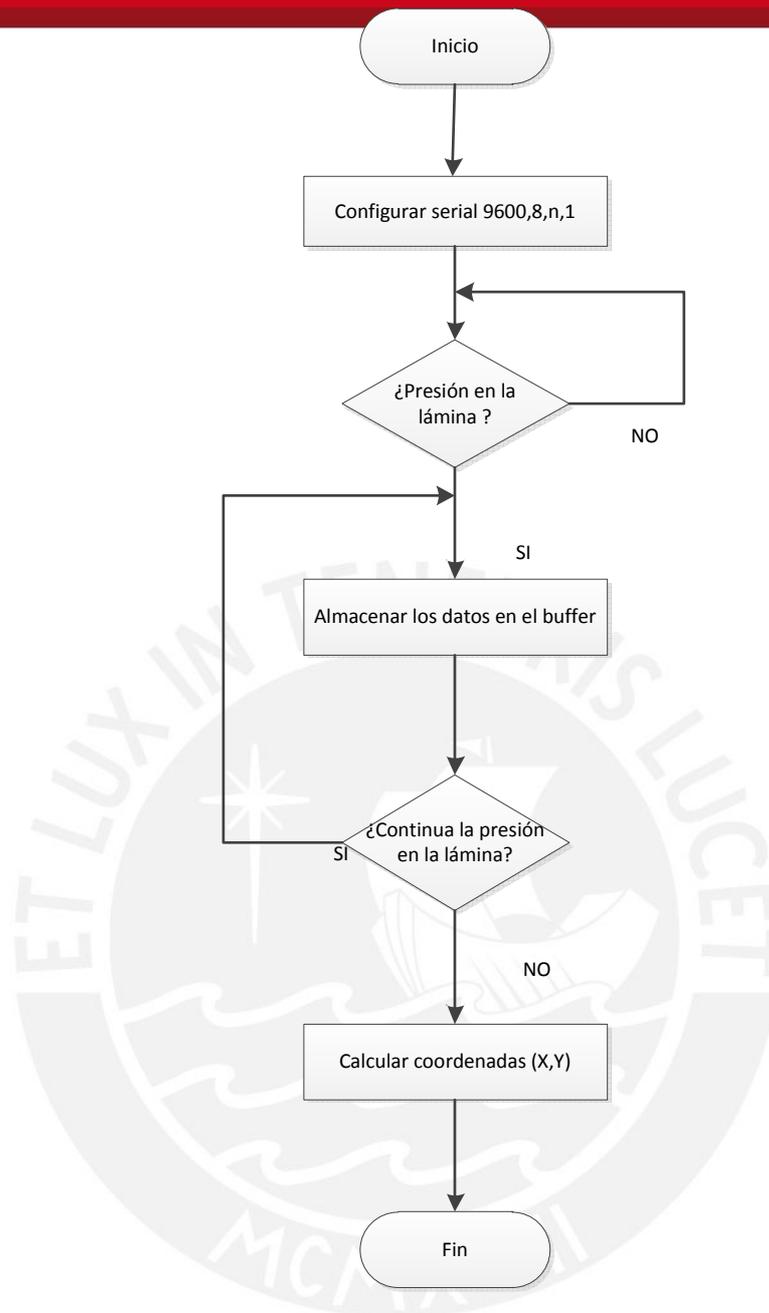


Diagrama N° 3.1 Flujo de Adquisición de datos de la lámina táctil

Mientras exista presión sobre un punto de la lámina táctil, su controlador transmite constantemente 5 bytes a 9600, 8 bit de datos, sin paridad y un bit de fin. El primer byte indica si existe presión o no sobre la lámina, mientras que los 4 bytes restantes indican las coordenadas (x,y) del punto de presión. Los datos se almacenan en un buffer de memoria RAM y con estos se calcula las coordenadas del punto de presión.

### 3.2 Configuración de la Cédula de votación

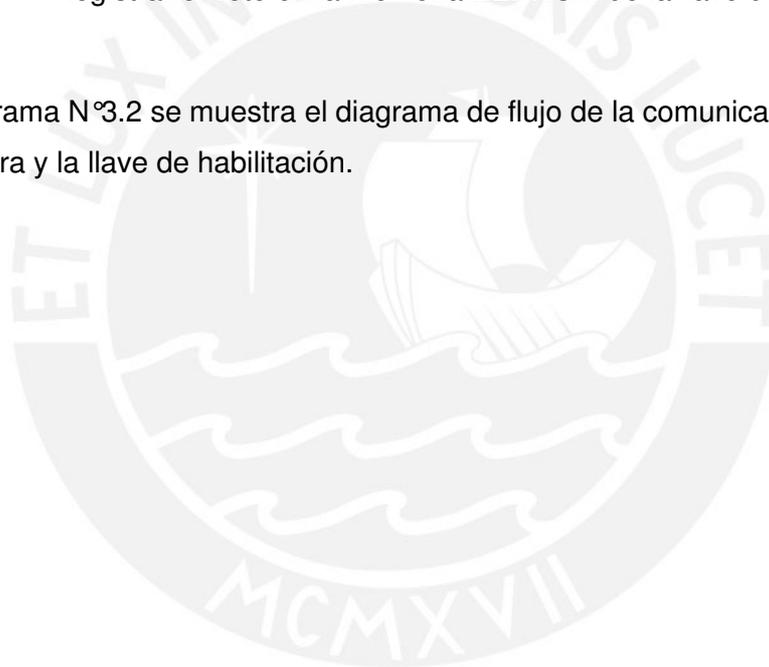
Permite configurar la disposición de las zonas activas de presión, mediante la grabación de las coordenadas de los rectángulos, los cuales definen las áreas de presión con las opciones mostradas en la cédula de votación. Las coordenadas de los rectángulos se almacenan en la memoria EEPROM del microcontrolador de la tarjeta controladora.

### 3.3 Comunicación equipo – llave

Permite el Intercambio de información para:

- Obtener el estado de la llave de habilitación (activo, desactivo).
- Desactivar la llave inmediatamente después de ejecutado el voto.
- Registrar el voto en la memoria EEPROM de la llave de habilitación.

En el diagrama N°3.2 se muestra el diagrama de flujo de la comunicación entre la tarjeta controladora y la llave de habilitación.



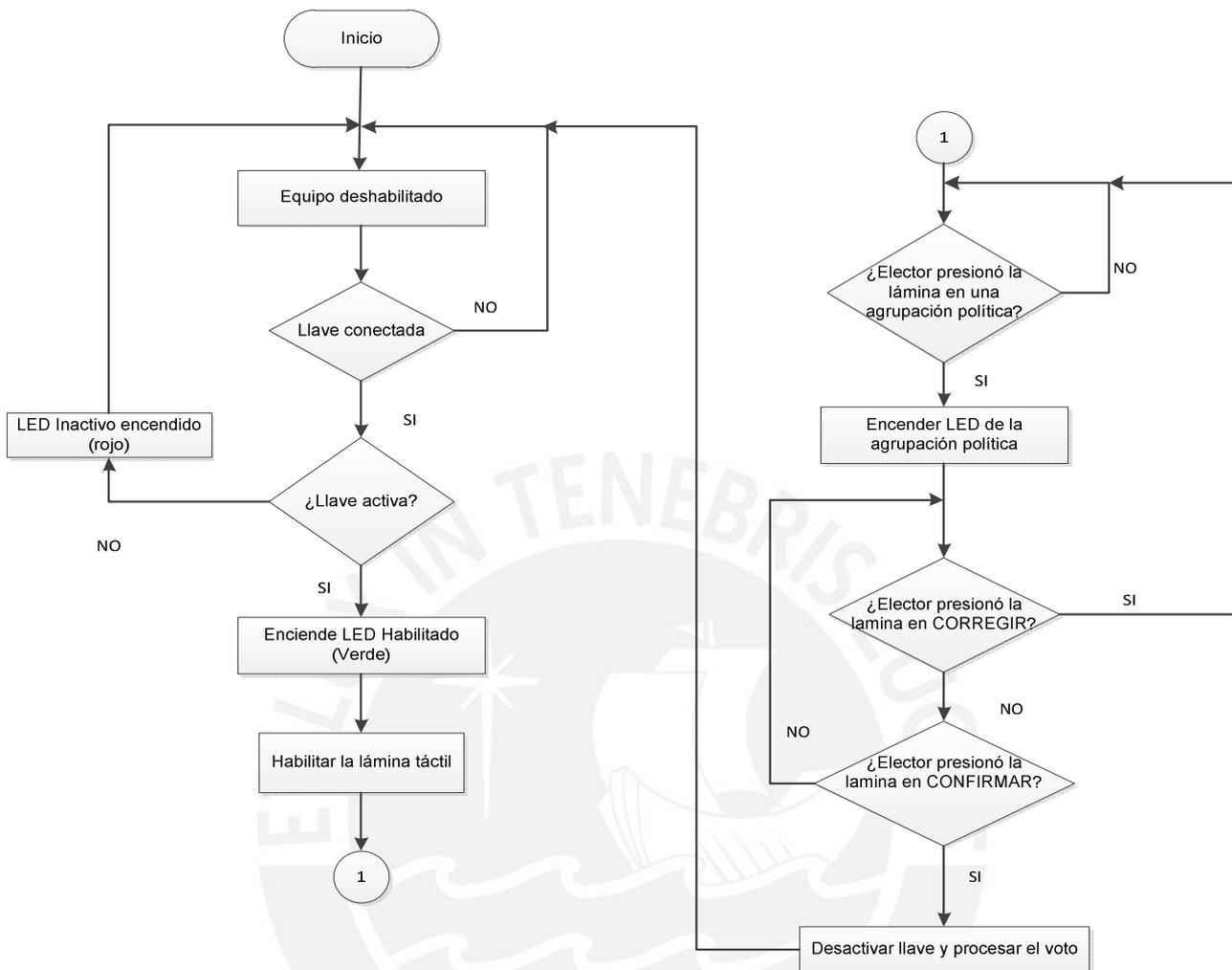


Diagrama N° 3.2 Flujo de Comunicación equipo – llave

Al introducir la llave de habilitación, la tarjeta controladora obtiene el estado de la llave, si la llave esta activada, entonces se habilita el equipo para poder votar, el elector selecciona su candidato, puede cambiar su elección o confirmarla, con lo cual se desactiva la llave y se procesa el voto.

### 3.4 Protocolo de comunicación sobre un pin

Para facilitar la conexión de una llave de habilitación con el equipo de voto electrónico, se utiliza un conector de audio (plug stereo), debido a que sólo tiene una posición para la conexión, facilitando su uso al elector. El plug de audio stereo tiene 3 contactos, los cuales se usan para energizar la tarjeta de llave de habilitación y el tercer contacto se

utiliza como un canal de comunicación. En el canal de comunicación se implementa un protocolo serial asíncrono [13], half dúplex, es decir, la transmisión y recepción no se realiza en forma simultánea, en un momento un microcontrolador transmite mientras el otro recibe los datos y viceversa.

Para la recepción de datos se utiliza la interrupción externa por flanco de bajada y un temporizador con interrupción por comparación para obtener el valor del bit presente en la línea.

Para la transmisión de datos se utiliza la misma interrupción por comparación para colocar el valor del bit en la línea. Para discriminar entre una transmisión y una recepción se utiliza una variable **contador**, la cual indica que se está realizando una transmisión de datos cuando su valor es un número par, y cuando es impar, se está realizando una recepción de datos [19]. La Figura 3.1 muestra los valores que toma la variable contador.

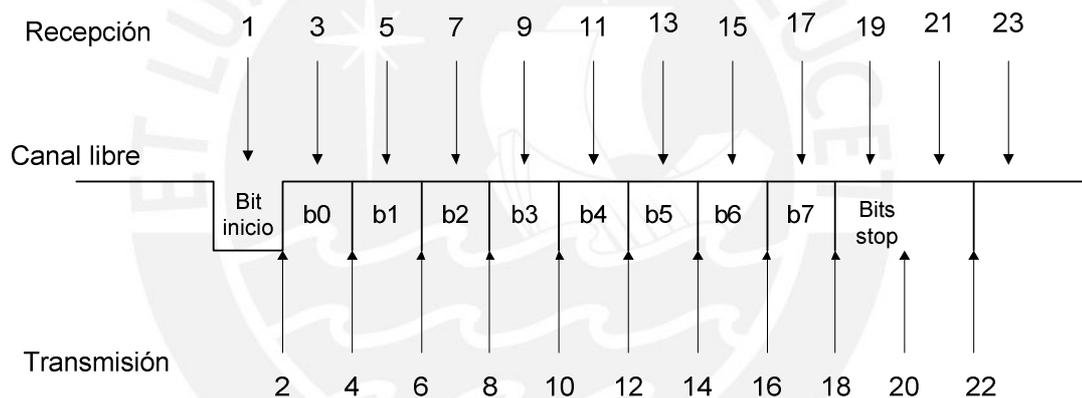


Figura 3.1 Muestreo de bits

Para la recepción de datos, se configura en la rutina de servicio de interrupción por interrupción externa, el registro de comparación del temporizador, para realizar el muestreo en el punto medio del primer bit de datos recibido (b0). En la rutina de servicio de interrupción, de la primera interrupción por comparación, se reconfigura el registro de comparación al valor de un tiempo de bit, con lo cual las siguientes interrupciones del temporizador muestrearán el valor del bit en el punto medio.

Para la transmisión de datos, se configura el registro de comparación del temporizador al valor tal que la primera interrupción por comparación ocurra un tiempo de bit después del inicio del bit de inicio y a partir de este momento las siguientes interrupciones por comparación ocurrirán cada un tiempo de bit.

El pin del puerto por el cual se comunican los datos seriales tiene una resistencia de 10 K $\Omega$  conectada a 5 V. (resistencia en pull - up) en la tarjeta Controladora. Una vez que se conecta la tarjeta Llave de habilitación, se tienen conectados ambos pines que forman el canal de comunicación. El dispositivo transmisor pone la línea a 0 voltios indicando el inicio de la transmisión (bit de inicio), mientras que el receptor procesa este cambio del valor de la línea como una interrupción externa por flanco de bajada.

En la programación realizada en lenguaje ensamblador se divide el código de acuerdo a las siguientes tareas:

- Habilitación de la comunicación asíncrona (Diagrama N° 3.3)
- Función de transmisión (Diagrama N° 3.4)
- Función de recepción (Diagrama N° 3.5)
- Rutina de Interrupción Externa (Diagrama N° 3.6)
- Rutina de Interrupción del Temporizador por comparación (Diagrama N° 3.7)
- Manejador de la transmisión (Diagrama N° 3.8)
- Manejador de la recepción (Diagrama N° 3.9)

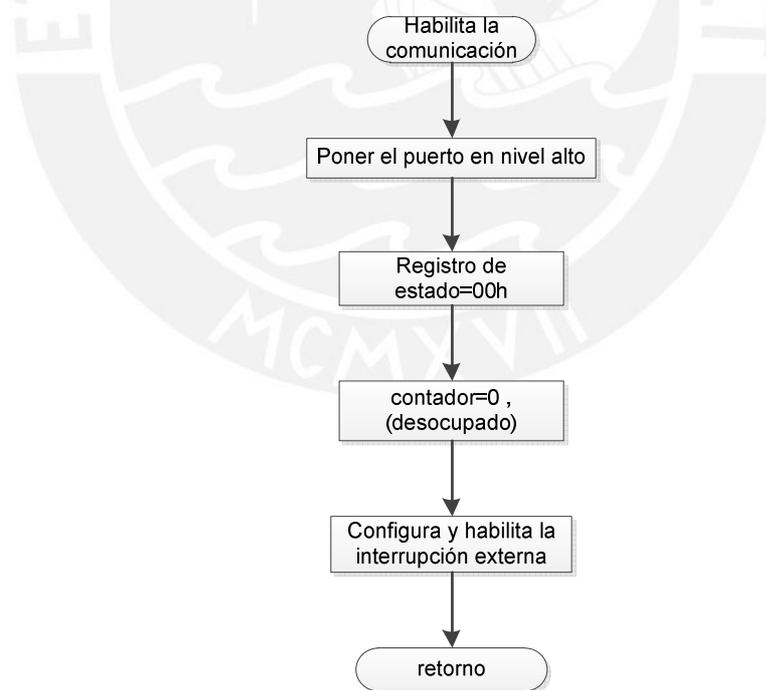


Diagrama N° 3.3 Flujo de habilitación de la comunicación

La habilitación de la comunicación consiste en la configuración de las condiciones iniciales al inicio de la comunicación.

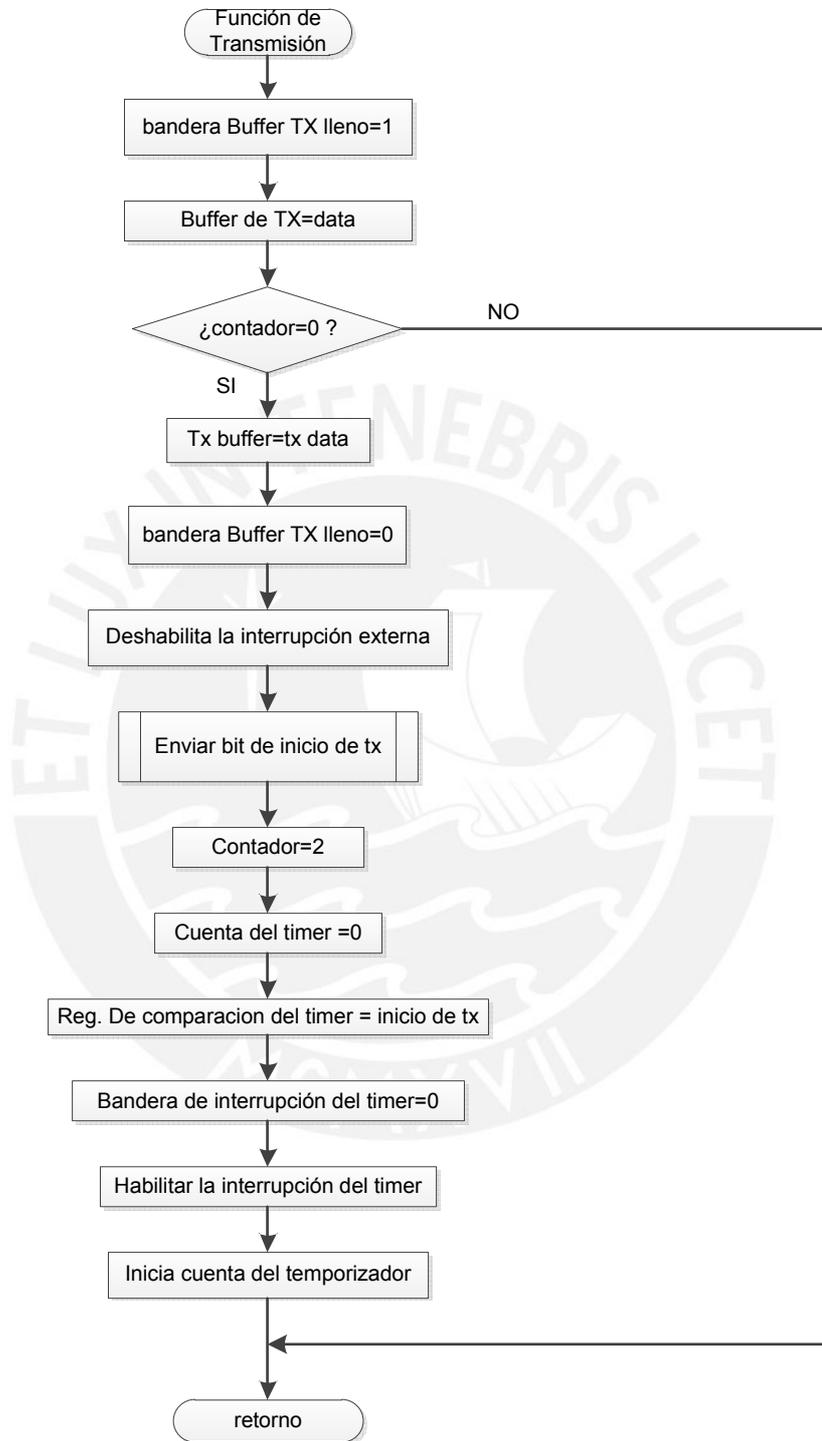
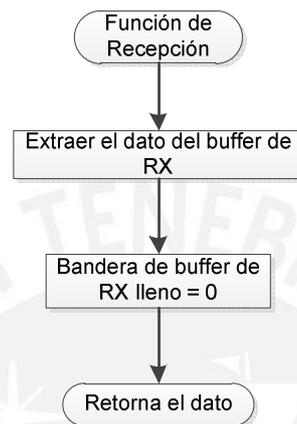


Diagrama N° 3.4 Flujo de la función de transmisión

La función de transmisión coloca el byte a transmitir en un buffer de transmisión, deshabilita la interrupción externa, dado que los bits en nivel bajo producirían interrupciones externas, coloca en la línea un nivel bajo indicando el inicio de la transmisión, es decir, el bit de inicio, y configura el temporizador para interrumpir al final del bit de inicio.



La función de recepción extrae el byte recibido (el cual se obtuvo a través de interrupciones) leyendo la bandera que indica que hay un dato en el buffer de recepción.

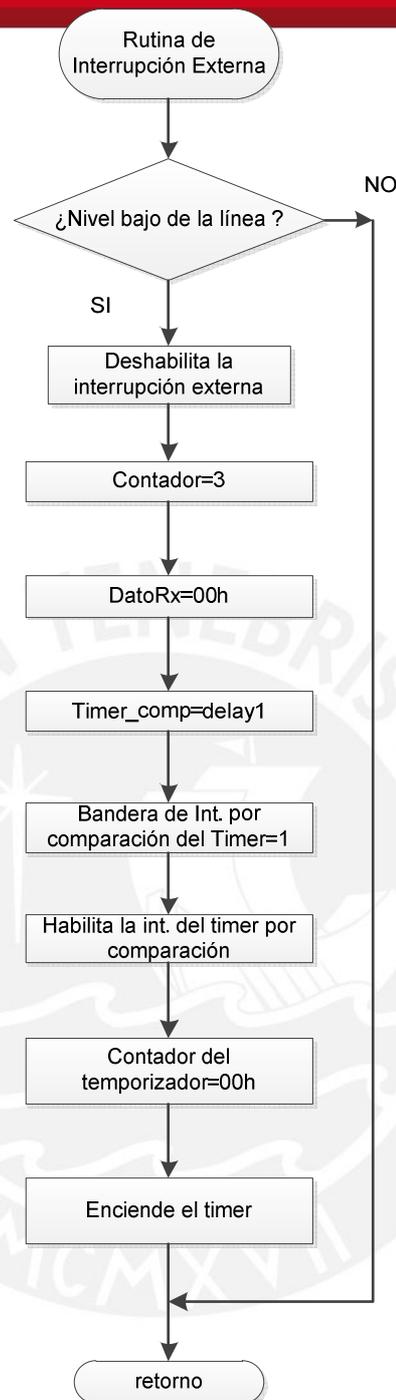


Diagrama N° 3.6 Flujo de la rutina de interrupción externa

La rutina de interrupción externa verifica que el nivel de la línea sea bajo, esto indica que se tiene el bit de inicio, deshabilita la interrupción externa, dado que los bits en 0 generarían interrupciones externas y configura la interrupción del temporizador para que se produzcan interrupciones cada un tiempo de bit.

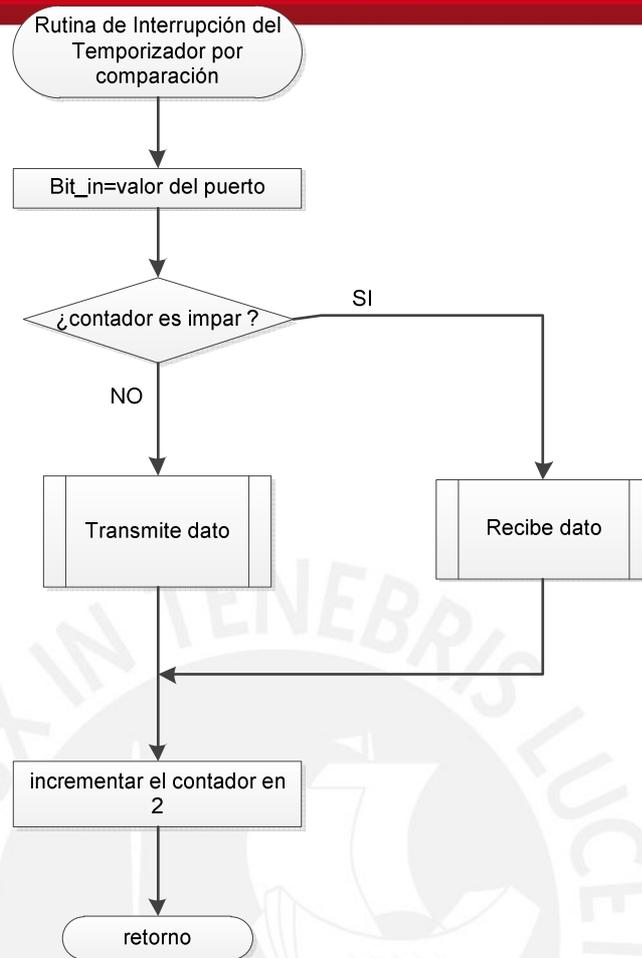


Diagrama N° 3.7 Flujo de la rutina de interrupción del temporizador por comparación

La rutina de interrupción del temporizador realiza una lectura del pin de comunicación en la variable “bit\_in” luego discrimina si se está transmitiendo o recibiendo bits, esto a través de la lectura de la variable contador. Si el valor de la variable contador es un número impar, entonces se están recibiendo bits y si es par se están transmitiendo.

La función Transmite Dato maneja la transmisión de bits, mientras que la función Recibe Dato maneja la recepción de bits.

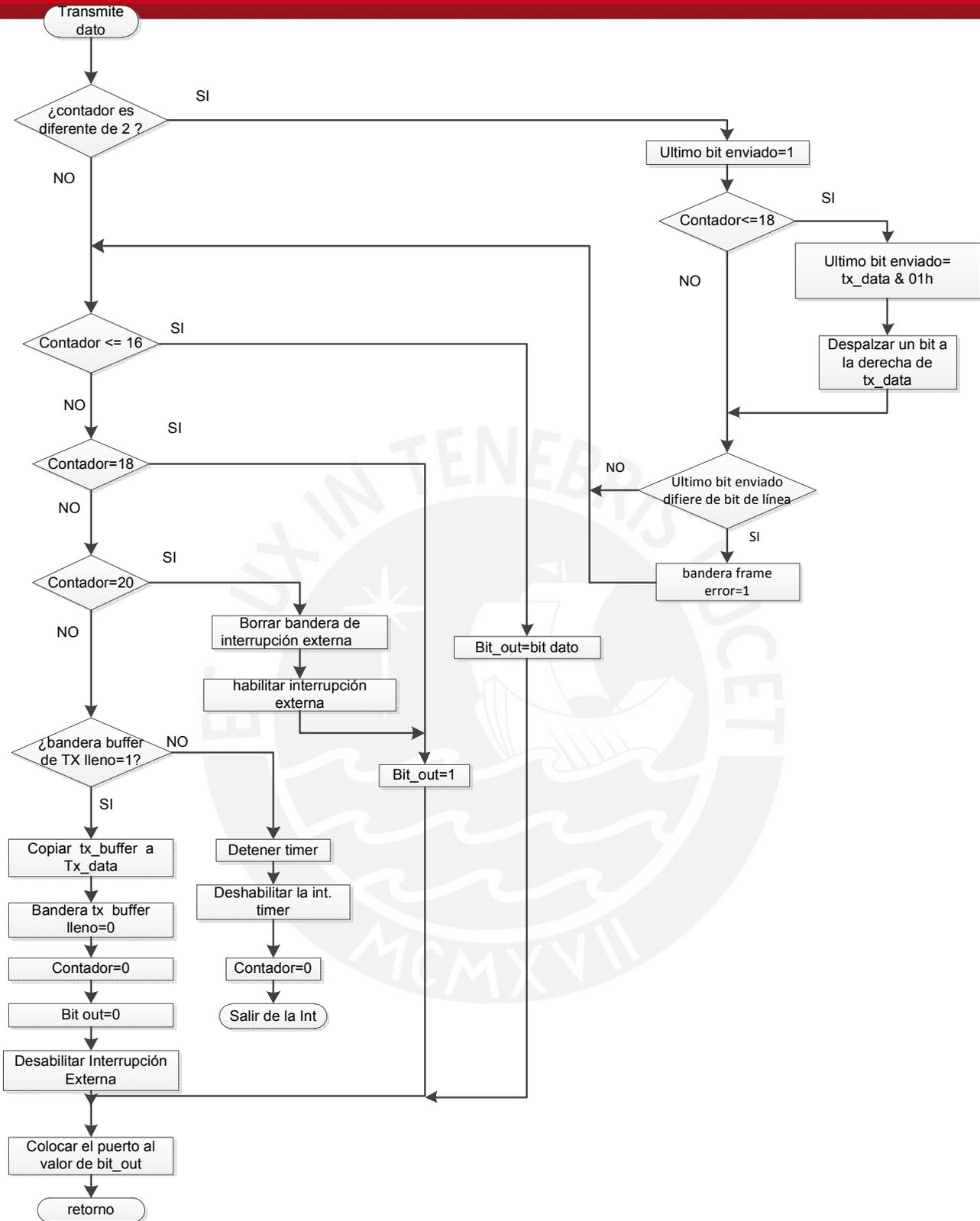


Diagrama N° 3.8 Flujo del manejador de la transmisión

La función “Transmite dato”, la cual está incluida en la rutina de servicio de interrupción del temporizador, coloca el valor de cada bit del byte de dato en el pin de comunicación.

En el pin se comunicación se coloca el valor de cada bit comenzando por el LSB del byte de dato, luego el byte de dato se desplaza un bit a la derecha. Se lleva el control de la cantidad de bits con la variable “contador”, la cual comienza con su valor en 2 para el primer bit (b0) hasta el valor 16 para el octavo bit (b8). Cuando la variable “contador” tiene los valores 18 y 20, se coloca en el pin un bit en 1 por cada uno, es decir, 2 bits de fin. La función antes de colocar el valor del bit actual, verifica si el valor del pin de comunicación capturado anteriormente en la rutina de servicio de interrupción del temporizador es igual al valor del último bit colocado en el pin, si son diferentes valores, entonces se indica a través de la bandera FE=1 del registro de estado que existe un error de trama. Si existe otro dato en el buffer, indicado por la bandera “buffer\_tx”=1, entonces se inicia otra transmisión, de no ser así, se sale de la rutina de servicio de interrupción del temporizador.



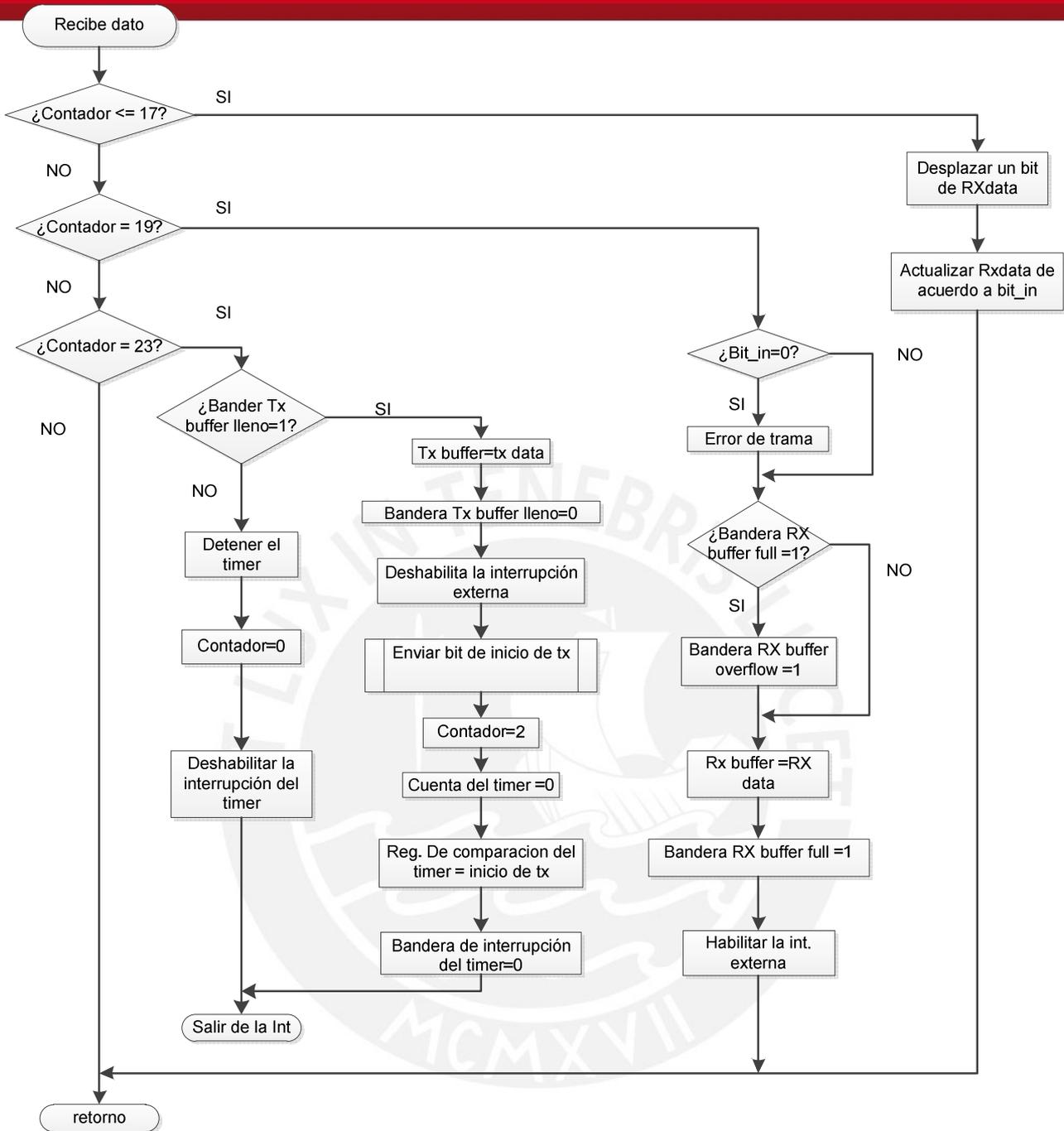


Diagrama N° 3.9 Flujo del manejador de la recepción

La función “Recibe dato”, la cual está incluida en la rutina de servicio de interrupción del temporizador, desplaza hacia la izquierda los bits de la variable “RXdata”, luego según el valor del pin de comunicación actualiza este valor en el bit LSB de la variable “RXdata”. Se lleva el control de la cantidad de bits con la variable “contador”, la cual comienza con su valor en 3 para el primer bit (b0) hasta el valor 17 para el octavo bit (b8).

Cuando la variable “contador” tiene el valor de 19 se verifica que el valor del pin de comunicación tenga un estado en alto, el cual indica que este es el bit de fin, indicando

que se tiene un dato por recoger del buffer de recepción a través de la bandera Rx buffer full. Si el valor del pin de comunicación es bajo, se indica a través de una bandera que existe un error de trama. Si al leer la bandera “Rx buffer full” su valor es 1, entonces se indica un “Rx buffer overflow”.

Cuando la variable “contador” tiene el valor de 23 se lee la bandera “Tx buffer full” para saber si hay algún dato por transmitir, si es así se inicia la transmisión del dato, caso contrario se deshabilita la interrupción del temporizador y se sale de la rutina de servicio de interrupción del temporizador.

### Determinación de la velocidad de transmisión

La velocidad de transmisión se define como la cantidad de bits transmitidos en un segundo, esto incluye el bit de inicio y los bits de fin. Ambos dispositivos (Transmisor y Receptor) deben estar configurados con los mismos parámetros para poder comunicarse.

$$\text{Velocidad de Transmisión (bps)} = \frac{\text{frecuencia del sistema}}{(\text{valor del registro de comparación del timer} + 1) * \text{prescalador}}$$

La frecuencia del cristal utilizado es de 4 MHz. Se ha configurado el registro de comparación del Temporizador (OCR0A) con el valor de 416 y el prescalador igual a 1, con lo cual se obtienen:

$$\text{Velocidad de Transmisión (bps)} = \frac{4\text{Mhz}}{(416 + 1) * 1} = 9592.32 \text{ bps}$$

El protocolo de transmisión de datos serial, es utilizado de la misma manera en ambos extremos de la comunicación, es decir, se implementa en la tarjeta Controladora y en la tarjeta Llave de habilitación de voto, por lo que ambos utilizan la misma velocidad de transmisión de 9592.32 bps.

En el caso particular que necesitemos comunicarnos con otro dispositivo que tenga por parámetros 9600 bits por segundo, el error porcentual sería:

$$\text{Error [\%]} = \left( \frac{\text{Velocidad de Transmisión más cercana (bps)}}{\text{Velocidad de Transmisión (bps)}} - 1 \right) * 100\%$$

$$\text{Error [\%]} = \left( \frac{9592.32 \text{ bps}}{9600 \text{ bps}} - 1 \right) * 100\% = - 0.08\%$$

La velocidad de transmisión máxima está limitada por el menor valor del registro de comparación del temporizador, de tal forma que la rutina de servicio de interrupción termine de ejecutarse antes que la siguiente interrupción ocurra. El número de ciclos mínimo que necesita la interrupción del temporizador es de 100, con lo cual la velocidad de transmisión máxima será de:

$$\text{Velocidad de Transmisión Máxima (bps)} = \frac{4\text{Mhz}}{(100 + 1) * 1} = 39603 \text{ bps}$$

Sin embargo al utilizar valores cercanos a la velocidad de transmisión máxima, la comunicación consumiría demasiados recursos de la CPU, por lo que se usa una menor velocidad de transmisión de 9592.32 bps.



## 4 IMPLEMENTACIÓN DEL SOFTWARE

Como parte de la solución de voto electrónico presencial, se necesita un equipo operado por un miembro de mesa, que tenga la función de identificar al elector. Este equipo usa aplicaciones de software que permiten identificar al elector a través de su foto, utilizando como dato el número del documento nacional de identidad (DNI), el cual está incluido en una base de datos correspondiente a la mesa de votación. Cuando se verifica que los datos del elector pertenecen a la mesa de votación, se activa la llave habilitadora y se le entrega al elector para que sólo pueda votar una única vez.

Como alcance del presente trabajo se contempla la activación y desactivación de la llave habilitadora, el registro de los votos y la presentación de resultados electorales. La identificación del elector no es parte del alcance del presente trabajo.

### 4.1 Activación de la llave habilitadora

Se desarrolló una aplicación para una computadora personal sobre la plataforma del sistema operativo Windows, la cual se comunica con la tarjeta habilitadora a través del puerto serie usando el protocolo RS232. La aplicación fue desarrollada en el lenguaje de programación C++, utilizando el entorno de desarrollo Qt de la marca Nokia. La aplicación permite activar un sólo voto y mostrar los resultados electorales al finalizar las elecciones en la mesa de votación.

### 4.2 Aplicación de Voto Electrónico

La aplicación posee dos ventanas, la primera ventana permite ingresar al sistema si se tienen las credenciales correctas. La segunda ventana se muestra sólo si se han validado las credenciales.

La interfaz de la aplicación (segunda ventana) muestra la cédula electoral con las agrupaciones políticas, sus símbolos y la cantidad de votos que obtuvieron en la jornada electoral. Al inicio de la jornada electoral cada contador de cada agrupación política indica 0 (cero) votos.

Existe un procedimiento denominado “Puesta a Cero”, el cual coloca todos los contadores de votos a cero votos, en los registros correspondientes.

La información electoral de los resultados es almacenada en un archivo, el cual es almacenado en el disco duro de la computadora portátil.

La interfaz posee tres botones con las siguientes funciones:

- Botón PUESTA A CERO, permite colocar todos los contadores de votos a cero votos.
- Botón ACTIVAR, permite activar la llave habilitadora para poder realizar un sólo voto.
- Botón RESULTADOS ELECTORALES, permite mostrar el estado de los contadores de votos

La figura 4.1 muestra la interfaz de verificación de credenciales y la Figura 4.2 muestra los resultados electorales, obtenidos de la llave de habilitación, a través del puerto de comunicación serial asíncrono.

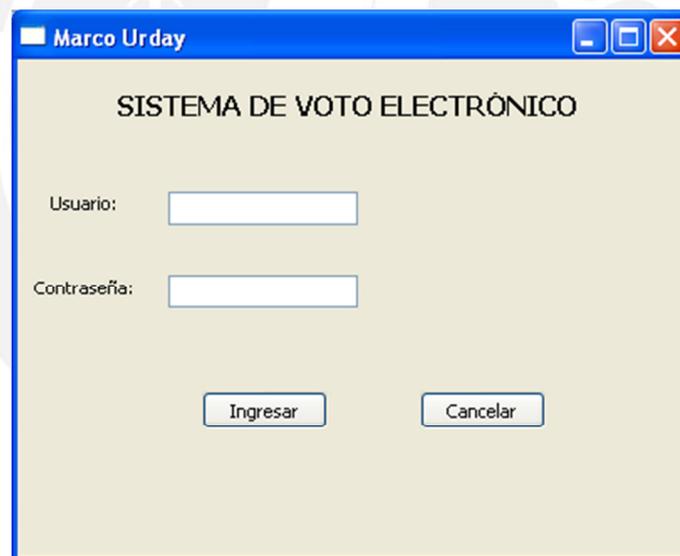


Figura 4.1. Imagen de la interfaz de verificación de credenciales



Figura 4.2 Resultados electorales

## 5 INTEGRACIÓN E IMPLEMENTACIÓN DEL PROTOTIPO

En el diseño e implementación de la tarjeta habilitadora, se buscó obtener el menor espacio, dado que debía empaquetarse en el chasis de un plug de audio. La tarjeta controladora se diseñó utilizando componentes superficiales. Los conectores utilizados permiten realizar un fácil mantenimiento al equipo. El chasis utilizado es de madera, debido a que este material tiene un menor costo en comparación al metal y permite realizar ligeros cambios, dado que la implementación corresponde a un prototipo.

### 5.1 Prototipo

Se define un prototipo como una versión operativa preliminar del proceso de construcción de un producto, para fines de demostración y evaluación. El prototipo se modifica por medio de un proceso iterativo que consiste en probar y modificar constantemente hasta que cumpla los requerimientos del producto.

El proceso iterativo se puede resumir en cuatro procesos:

- Análisis
- Diseño
- Implementación del prototipo
- Pruebas del prototipo

La Figura 5.1 muestra la imagen de la metodología cíclica, para el proceso de creación de un producto, en el cual se muestra el proceso iterativo de mejora continua del prototipo.



Figura 5.1 Metodología cíclica de un prototipo

## 5.2 Costos de la implementación del Prototipo

Los componentes del equipo se seleccionaron considerando el menor costo, peso y volumen. La mayoría de los componentes se compraron en el mercado local. El costo total del equipo de voto electrónico presencial es de 744.2 Nuevos Soles. En las siguientes tablas se detalla el costo por cada componente.

Tabla 5.1 Costo de la Tarjeta controladora

Costos de la tarjeta controladora						
	Componente	Origen	Descripción	Cantidad	Precio U. (S/.)	Subtotal (S/.)
1	PCB Controlador	local	fibra	1	77	77
2	MCU Atmega 88	local		1	13.5	13.5
3	Cristal de 4 MHz	local		1	1.5	1.5
4	Decoder 74HC154	importado		1	12	12
5	Regulador MCP1702	importado		1	3.3	3.3
6	IC MAX232	local		1	1	1
7	Zumbador	local		1	1.5	1.5
8	Resistencias	local		32	0.3	9.6
9	Condensadores	local		14	0.3	4.2
10	Conectores	local	jack,DB9	1	5	5
11	espadines	local	2x20	2	1	2
<b>Total 1</b>						<b>130.6</b>

Elaboración: propia

Tabla 5.2 Costo de la Tarjeta Habilitadora

Costos de la tarjeta habilitadora						
	Componente	Origen	Descripción	Cantidad	Precio U. (S/.)	Subtotal (S/.)
1	PCB Habilitador	local	fibra	1	7	7
2	MCU Atmega 88	local		1	13.5	13.5
3	Cristal de 4 MHz	local		1	1.5	1.5
4	IC MAX232	local		1	1	1
5	Resistencias	local		2	2	4
6	Condensadores	local		10	0.3	3
7	Conectores	local	Plug-audio	1	1	1
8	espadines	local	2x20	1	1	1
<b>Total 2</b>						<b>32</b>

Elaboración: propia

Tabla 5.3 Costo del Alojamiento mecánico

<b>Costos del Chasis</b>						
	<b>Componente</b>	<b>Origen</b>	<b>Descripción</b>	<b>Cantidad</b>	<b>Precio U. (S/.)</b>	<b>Subtotal (S/.)</b>
1	pilas NI-MH , AA 2100 mA	local		6	10	60
2	chasis de madera	local		1	50	50
3	pintura	local		1	30	30
4	carpintería	local		1	50	50
5	cables	local		1	3	3
6	cinta doble contacto	local		1	6	6
7	diodo emisor de luz (LED)	local		13	0.2	2.6
8	bisagras	local		2	1.5	3
9	silicona	local		2	1	2
					<b>Total 3</b>	<b>206.6</b>

Elaboración: propia

Tabla 5.4 Costo de la lámina táctil

	<b>Componente</b>	<b>Origen</b>	<b>Descripción</b>	<b>Cantidad</b>	<b>Precio U. (S/.)</b>	<b>Subtotal (S/.)</b>
1	Lamina táctil y controlador	importado		1	305	305
					<b>Total 4</b>	<b>305</b>

Elaboración: propia

Tabla 5.5 Costo de los servicios

	<b>Componente</b>	<b>Origen</b>	<b>Descripción</b>	<b>Cantidad</b>	<b>Precio U. (S/.)</b>	<b>Subtotal (S/.)</b>
1	ensamblaje	local		1	50	50
2	logística	local		1	20	20
					<b>Total 5</b>	<b>70</b>

Elaboración: propia

Tabla 5.6 Costo del Equipo de voto electrónico

	<b>Componente</b>		<b>Subtotal (S/.)</b>
1	Tarjeta controladora		130.6
2	Tarjeta habilitadora		32
3	Chasis y pilas		206.6
4	Lámina táctil		305
5	ensamblaje y logística		70
		<b>Total (S/.)</b>	<b>744.2</b>

Elaboración: propia

El costo de ingeniería asciende a S/. 12000 considerando 640 horas de trabajo. El costo de ingeniería incluye el desarrollo del software.

La figura 5.2 muestra el equipo de voto electrónico implementado.



Figura 5.2 Fotografía del equipo de voto electrónico

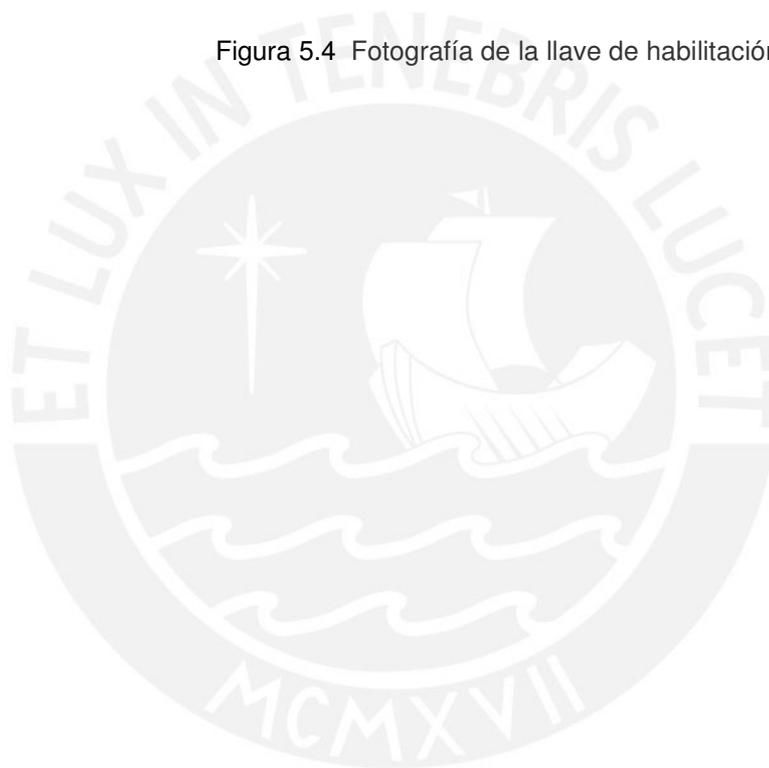
La figura 5.3 muestra la tarjeta controladora fabricada y la figura 5.4 muestra la tarjeta llave de habilitación en la que se aprecia el conector de audio.



Figura 5.3 Fotografía de la Tarjeta Controladora



Figura 5.4 Fotografía de la llave de habilitación



## 6 SEGURIDAD DE LA INFORMACIÓN

La información es un activo que tiene valor para la organización y requiere una protección adecuada [14]. La seguridad de la información protege la información de un amplio rango de amenazas, para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios.

### 6.1 Características de la Seguridad de la información

#### Preservación de la:

- **Confidencialidad**, propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados. [15]
- **Integridad**, propiedad de salvaguardar la exactitud y completitud de los activos. [15]
- **Disponibilidad**, propiedad de ser accesible y utilizable por una entidad autorizada. [15]

La seguridad de la información es un componente principal de la solución de voto electrónico, ya que permite preservar la confidencialidad, la integridad y la disponibilidad de la información del proceso electoral.

#### Definiciones:

- **Activo**. Algo que tenga valor para la organización [15].
- **Amenaza**. Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización. [15]
- **Vulnerabilidad**. Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas. [15]
- **Riesgo**. Combinación de la probabilidad de un evento y sus consecuencias. [16]

- **Control.** Herramienta de la gestión del riesgo, incluyendo políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal.

## 6.2 Análisis de Riesgo del equipo de voto electrónico

- **Vulnerabilidad.** Las tramas de comunicación entre la tarjeta controladora y la llave de habilitación, del equipo de voto electrónico presencial, fluyen en texto plano, es decir, sin cifrar.
- **Amenaza.** Intercepción, análisis y emulación de las tramas de comunicación entre la tarjeta controladora y la llave de habilitación.
- **Riesgo.** Al replicar el hardware de la llave de habilitación y realizar más de un voto, el sistema de votación electrónica perdería la confianza de los electores en la realización de elecciones que reflejen la voluntad popular.
- **Control.** Realizar una encriptación del canal de comunicación entre la tarjeta controladora y la llave de habilitación.

## 6.3 Criptografía

### Definición

Técnicas que permite la alteración de las representaciones lingüísticas de un mensaje.

Se aplica en la protección de la información, para que esta no sea accesible por observadores no autorizados.

### Aplicaciones

- **Secreto:** Modificar un mensaje para que se transforme en otro completamente ilegible si no se tiene la clave con la que fue modificado el mensaje original.
- **Control de integridad:** Verifica que la información no ha sido alterada intencionalmente.
- **Validación de la identificación:** Determinar con quien se está comunicando, antes de revelar la información.

### Tipos de Criptografía

- Criptografía Simétrica
- Criptografía Asimétrica

## Criptografía Simétrica

Utiliza algoritmos que usan la misma clave para cifrar y descifrar el mensaje plano.

El algoritmo RIJNDAEL es el más usado. Fue adoptado por el gobierno de los E.E.U.U como un estándar para la protección de datos. Este algoritmo es conocido como AES (Advanced Encryption Standard) y fue desarrollado por Vincent Rijmen y Joan Daemen.

## Criptografía Asimétrica

Utiliza algoritmos que usan una clave para cifrar y otra clave para descifrar el mensaje plano. El algoritmo RSA es el más utilizado y fue desarrollado por Rivest, Shamir y Adleman.

Criptoperíodo es el lapso de tiempo durante el cual se autoriza una clave específica para su uso legítimo. Un criptoperíodo adecuado limita el tiempo disponible para ataques criptográficos de cómputo intensivo.

La complejidad computacional, definida como el tiempo que tarda un computador para realizar una tarea (tiempo que tarda en procesar un algoritmo)

En criptografía la complejidad computacional es importante desde dos puntos de vista:

- Interesa que los algoritmos de encriptación, desencriptación y elección de claves requieran poco tiempo de cálculo.
- Cualquier algoritmo de desencriptación, suponiendo no conocida la clave, requiere un alto costo computacional.

El costo computacional de un algoritmo depende de:

- El propio algoritmo, en cuanto al número de operaciones a realizar y el tipo de operaciones que tiene que realizar.
- La computadora sobre la cual se está ejecutando el algoritmo.

## Ataque de fuerza bruta

Implica intentar cada clave posible hasta que se obtenga la traducción legible del texto cifrado al texto plano. En la siguiente Tabla N° 6.1 se muestra la relación entre el tamaño de la clave para una criptografía simétrica y el tiempo necesario para realizar un ataque de fuerza bruta. [17]

Tabla N° 6.1 Longitud de clave simétrica vs permutaciones

tamaño de la clave en bits	Permutaciones	Tiempo para un ataque de fuerza bruta para un dispositivo que realiza $2^{56}$ permutaciones por segundo
8	$2^8$	0.001 milisegundos
40	$2^{40}$	0.015 milisegundos
56	$2^{56}$	1 segundo
64	$2^{64}$	4 minutos 16 segundos
128	$2^{128}$	149,745,258,842,898 años
256	$2^{256}$	50,955,671,114,250,072,156,962,268,275,658,377,807,020,642,877,435,085 años

Elaboración: [17]

Tabla N° 6.2 Tamaño mínimo en bits de la clave simétrica para diferentes atacantes [18]

Atacantes	Presupuesto	Hardware	Seguridad mínima
"Hacker"	0	PC	53
	< \$400	PC(s)/FPGA	58
	0	"Malware"	73
Organización pequeña	\$10K	PC(s)/FPGA	64
Organización pequeña	\$300K	FPGA/ASIC	68
Organización grande	\$10M	FPGA/ASIC	78
Agencia de Inteligencia	\$300M	ASIC	84

Elaboración: [18]

Tabla N° 6.3: Equivalencia entre tamaños de clave simétrica vs asimétrica

Seguridad (bits) (Criptografía Simétrica)	RSA (Criptografía Asimétrica)
48	480
56	640
64	816
80	1248
112	2432
128	3248
160	5312
192	7936
256	15424

Seguridad (bits) (Criptografía Simétrica)	RSA (Criptografía Asimétrica)
50	512
62	768
73	1024
89	1536
103	2048

Elaboración: [18]

Para el presente trabajo, se consideró como parte del diseño de la seguridad, el uso de un algoritmo de clave simétrica, debido a que estos algoritmos tienen como característica una fácil implementación, en comparación con los algoritmos de clave asimétrica que son más complejos y utilizan un mayor tiempo de cómputo. Se usará el algoritmo RIJDAEL (desarrollado por Vincent Rijmen y Joan Daemen) adoptado como un estándar y conocido como AES (Advanced Encryption Standard). Este algoritmo permitirá cifrar el canal de comunicaciones, entre el equipo de voto electrónico y la llave habilitadora para proteger la información transmitida. Para determinar la longitud de la clave se adopta la recomendación del NIST (National Institute of Standards and Technology), cuando indica que las 3 longitudes de claves (128 bit, 192 bits y 256 bits) para el AES proveen una adecuada encriptación hasta el año 2031. La longitud de la clave a usarse es de 256 bits para lograr un cifrado muy fuerte y prácticamente imposible de romper ante un ataque de fuerza bruta.

Además de la elección del algoritmo de encriptación y la longitud de la clave, se debe implementar lo siguiente:

- Protección de los equipos de voto electrónico mediante un control físico,
- Protección de la clave de encriptación mediante procedimientos de control físico y lógico.

El tiempo de vida de la clave de encriptación en un proceso electoral, para la solución de voto electrónico, es igual al tiempo entre el inicio del proceso electoral y su finalización en la mesa de votación, disminuyendo la probabilidad de un ataque al sistema.

La implementación del algoritmo de encriptación AES 256 sobre el canal de comunicación entre el equipo de voto electrónico y la llave habilitadora no es parte del alcance del proyecto, sin embargo su implementación posterior corresponderá a una mejora al sistema.

## CONCLUSIONES

- Se implementó un equipo de voto electrónico presencial de bajo costo, portátil, de bajo peso, con energía proveída por un arreglo de 6 pilas comerciales de 1.2 V cada una.
- El equipo permite demostrar que una solución específicamente diseñada para una particular función (embedded system) es una opción viable para la implementación del voto electrónico en el Perú.
- La arquitectura del hardware implementado permite la realización de auditorías.
- El peso aproximado del equipo es: 4 Kg, facilitando su transporte y almacenamiento.

## RECOMENDACIONES

- El equipo diseñado debe ubicarse en un proceso de mejora continua, hasta que se obtenga un producto estable, el cual pueda ser fabricado a gran escala.
- El equipo de voto electrónico presencial es vulnerable ante una interceptación, análisis y emulación de las tramas de comunicación entre la tarjeta controladora y la llave de habilitación. Para minimizar el riesgo de replicar el hardware de la llave de habilitación y realizar más de un voto, se debe realizar una encriptación del canal de comunicación.
- El equipo de voto electrónico implementado debe ser probado en diferentes climas y alturas del territorio nacional, en las zonas en donde se realizan elecciones, para observar su comportamiento.

## BIBLIOGRAFÍA

- [1] Voto Electrónico – Preguntas Frecuentes  
  
<http://www.web.onpe.gob.pe/voto-electronico.html>  
  
consulta: Marzo 2012
- [2] Objetivos del voto electrónico  
  
<http://www.web.onpe.gob.pe/voto-electronico.html>  
  
Consulta: Marzo 2012
- [3] Aspectos tecnológicos del voto electrónico  
  
PANIZO ALONSO, LUIS  
  
Lima: ONPE, 2007  
  
<http://www.web.onpe.gob.pe/modEscaparate/downloads/l-2-2-017.pdf>
- [4] Servicio de Consultoría de Hardware  
  
<http://www.web.onpe.gob.pe/modAdquisiciones/downloads/2008/BASESSE RVCONSULTORIAHARDWAREver05.doc>  
  
Consulta: Marzo 2012
- [5] Servicio de Elaboración de Prototipo para equipo de voto electrónico  
  
[http://docs.seace.gob.pe/mon/docs/procesos/2009/000027/000027\\_EXO-3-2009-ONPE-BASES.doc](http://docs.seace.gob.pe/mon/docs/procesos/2009/000027/000027_EXO-3-2009-ONPE-BASES.doc)  
  
Consulta: Marzo 2012
- [6] Segunda Elección Presidencial 2011, en el distrito de Pacarán, provincia de Cañete, departamento de Lima.

<http://www.voto-electronico.org/category/pa%C3%ADs/per%C3%BA>

Consulta: Marzo 2012

- [7] Touch Screen Technology Comparison

<http://www.ieeinc.com/touch-screen-technology-comparison>

Consulta: Marzo 2012

- [8] Comparative Study of Various Touchscreen Technologies

<http://www.ijcaonline.org/volume6/number8/pxc3871433.pdf>

Consulta: Marzo 2012

- [9] Hojas Técnicas del regulador Microchip MCP-1702

<http://ww1.microchip.com/downloads/en/DeviceDoc/21983A.pdf>

Consulta: Marzo 2012

- [10] Hojas Técnicas de la batería recargable

<http://www.gpbatteries.com/pic/GP210AAHC.pdf>

Consulta: Marzo 2012

- [11] Atmel AVR042: AVR Hardware Design Considerations

<http://www.atmel.com/Images/doc2521.pdf>

Consulta: Marzo 2012

- [12] Hojas Técnicas del circuito integrado MAX232

<http://datasheets.maxim-ic.com/en/ds/MAX220-MAX249.pdf>

Consulta: Marzo 2012

- [13] Protocolo RS2332

[http://www.radio-electronics.com/info/telecommunications\\_networks/rs232/eia-rs232-c-d-standards.php](http://www.radio-electronics.com/info/telecommunications_networks/rs232/eia-rs232-c-d-standards.php)

Consulta: Marzo 2012

- [14] Standar ISO/IEC 17799:2005

Information Technology – Code of practice for information Security Management

<http://www.pecert.gob.pe/media/uploads/isoiec17799.pdf>

Consulta: Marzo 2012

- [15] Standar ISO/IEC 13335-1:2004

Information Technology - Security Techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.

Consulta: Marzo 2012

- [16] ISO/IEC Guide 73:2002

Risk management -- Vocabulary -- Guidelines for use in standards

consulta: Marzo 2012

- [17] Ataque de Fuerza Bruta

[http://en.wikipedia.org/wiki/Brute-force\\_attack](http://en.wikipedia.org/wiki/Brute-force_attack)

consulta: Marzo 2012

- [18] ECRYPT II Yearly Report on Algorithms and Keysizes (2010-2011) Table 7.1, Table 7.2, Table 7.3

<http://www.ecrypt.eu.org/documents/D.SPA.17.pdf>

consulta: Marzo 2012

- [19] AVR274: Single-wire Software UART

<http://www.atmel.com/Images/AVR274.pdf>

consulta: Marzo 2012

- [20] Hoja de datos del microcontrolador ATmega88PA

<http://www.atmel.com/Images/doc8271.pdf>

consulta: Marzo 2012

- [21] Hoja de datos del MOSFET canal N RK7002B

<http://www.rohm.com/products/databook/tr/pdf/rk7002b.pdf>

consulta: Marzo 2012

- [22] Observatorio de voto electrónico en Latinoamérica.

<http://www.voto-electronico.org/sites/default/files/reportes/brasil.pdf>

consulta: Marzo 2012

- [23] Tribunal Superior Electoral de Brasil – Adquisición de Urnas Electrónicas UE2010

## Especificación de Urna Electrónica Modelo 2010

Audiencia Pública 17894/2010 número de licitación 081/2010

<http://www.tse.jus.br/transparencia/licitacoes/licitacoes-concluidas>

consulta: Marzo 2012

- [24] Venezuela: Elecciones Parlamentarias 2010

<http://www.smartmatic.com/espanol/casos-de-estudio/view/article/venezuela-parliamentary-elections-2010/>

consulta: Marzo 2012

- [25] Máquina de votación táctil de Venezuela.

[http://www.smartmatic.com/fileadmin/users/docs/SAES/SAES-4000\\_ficha\\_tecnica\\_v4.0.pdf](http://www.smartmatic.com/fileadmin/users/docs/SAES/SAES-4000_ficha_tecnica_v4.0.pdf)

consulta: Marzo 2012

- [26] ¿Cuál es la mejor batería?

[http://batteryuniversity.com/learn/article/whats\\_the\\_best\\_battery](http://batteryuniversity.com/learn/article/whats_the_best_battery)

consulta: Marzo 2012

## ANEXOS

Disponible en el disco compacto