

---

UNIVERSIDAD POLITÉCNICA DE MADRID  
ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INDUSTRIALES  
DEPARTAMENTO DE AUTOMÁTICA, INGENIERÍA ELÉCTRICA Y ELECTRÓNICA E  
INFORMÁTICA INDUSTRIAL  
GRADO EN INGENIERÍA EN TECNOLOGÍAS INDUSTRIALES

TRABAJO FIN DE GRADO

# CERRADURA ELECTRÓNICA CON SISTEMA DE ALIMENTACIÓN INTEGRADO EN LLAVE

Alumno: **Enrique Manuel Garrote Sola**  
Tutores: **Jorge Portilla Berrueco**  
**Teresa Riesgo Alcaide**



Julio 2017



---

---

## **DEDICATORIA**

**Dedicado a mis padres, Manuel y María José, y a mis hermanos,  
Álvaro y María.**

---

---

## **AGRADECIMIENTOS**

Antes de nada, me gustaría agradecer a mis tutores, Jorge y Teresa, vuestro apoyo incondicional. A Teresa, por apoyarme en este proyecto desde la primera vez que te fui a ver, y siempre tener tiempo, incluso cuando no lo tenías, para reafirmar tu confianza en el proyecto y en mí y, a Jorge, por dejarme libertad para aprender y tomar las decisiones del proyecto, pero, a la vez, apoyarme y ayudarme siempre que lo he necesitado, compartiendo conmigo todo tu conocimiento y todas las herramientas que pudiera necesitar.

A mis padres, por todo lo que me habéis ayudado en este largo camino, incluso cuando no os dabais cuenta. Por retarme a tomar conciencia y a disfrutar de la libertad de quien se siente fruto de sus propias decisiones.

A mi padre, por enseñarme que el camino del esfuerzo no está remunerado, ni falta que hace.

A mi madre, por aguantarme y apoyarme siempre, incluso cuando piensas que estoy equivocado.

A mi hermana, por todo el cariño y la alegría que desprendes en todo lo que haces. Desde que naciste te he conocido así y, aunque ahora has guardado un poco la sonrisa, sé que siempre la llevas por dentro.

A mi hermano, por ser mi mejor defensor y por compartir la confianza que a todo hermano le gustaría tener.

A mi pareja, Beatriz, por ayudarme siempre a encontrar el ángulo muerto, ese punto de vista diferente que te permite dar un paso atrás y ver el mundo con ojos nuevos.

A mis abuelos, Diego y Tina, y a mi abuelo Pepe, lo que me habéis enseñado no está en ningún libro, y por eso roza el valor de lo incalculable. Sé que si estuvierais aquí os sentiríais orgullosos, porque una parte de este logro es, sin duda, vuestra también.

A mis mejores amigos de la escuela, Guti, Elena, Pablo, vosotros, incondicionales de domingos de biblioteca y de descansos cortos, pero a la vez, largos. Quizás, lo que menos tiempo sume de todo el que he pasado en la escuela sea el dedicado a esos descansos, pero, sin duda, es de ellos de donde acumulo mayores recuerdos, y, ojalá que sean muchos más.

A mis amigos de juventud, porque siempre son grandes los momentos que paso con vosotros, y sin esos grandes momentos, los demás no se podrían comparar.

---

---

## RESUMEN

Este proyecto pretende presentar una solución alternativa tanto para las cerraduras convencionales, como para aquellas electrónicas de reciente comercialización que, si bien suponen una mejora respecto a las primeras, no acaban de lanzar una propuesta sencilla que permita un uso generalizado.

Las cerraduras convencionales, basadas en elementos mecánicos, ofrecen una seguridad limitada que, aunque se ha incrementado mucho, empieza a ser difícil de mejorar. Por otro lado, las cerraduras electrónicas que se comercializan disponen de las mismas carencias de seguridad, ya que, o no acaban de prescindir de la cerradura mecánica o, la alternativa que ofrecen no acaba de mejorar la seguridad.

Se establece, por tanto, como objetivo principal de este proyecto, desarrollar un sistema de cierre electromecánico que consiga resolver las carencias de seguridad de los actuales sistemas. Siendo un objetivo ambicioso, se pretende poner en práctica las habilidades y capacidades desarrolladas por un estudiante de ingeniería industrial con vocación mecánica y electrónica.

Concretamente, los objetivos establecidos para el presente proyecto son los siguientes:

- Diseño y fabricación de un sistema de cierre electrónico con las siguientes características:
  - Accionamiento electromecánico
  - Posibilidad de instalación sobre plataformas existentes
  - Diseño orientado a futuras mejoras y modularidad
  - Bajo coste
- Fabricación de un prototipo funcional que permita la operación de una cerradura en condiciones de operación real.
- Programar el sistema para permitir la operación en condiciones reales, estableciendo la comunicación entre cerradura y llave y, sentando la base para desarrollos futuros.
- Dimensionar el par necesario para la operación de una puerta de seguridad mediante accionamientos electromecánicos, ofreciendo datos fiables para futuras consultas.

Se comienza el proyecto analizando el mercado y las soluciones existentes, llegando a la conclusión de la importancia de disponer de una alta fiabilidad, ya que cualquier fallo acabaría acarreado la imposibilidad de desbloquear el acceso. Con el fin de evitar esta situación pero

sin renunciar a los objetivos marcados, se decide adoptar una solución donde la energía quede integrada en la propia llave, permitiendo de esta manera una operación mucho más fiable debido, por un lado, a la ausencia de una conexión a la red eléctrica, lo que evitaría la inoperatividad del sistema en caso de fallo de suministro y, por otro, el reinicio del sistema tras cada operación garantiza la eliminación de cualquier error debido a un fallo en la ejecución.

Una de las ventajas fundamentales de esta solución es que se pretende integrar en el propio sistema de cierre de la puerta, utilizando los bulones propios de esta y, por tanto, disponiendo una seguridad tan elevada como aquella sea capaz de suministrar. Para lograrlo, se ha dimensionado un sistema de cierre habitual en una puerta de alta seguridad, analizando toda una serie de parámetros que influyen en el diseño y la selección de componentes. Este análisis es uno de los aspectos claves de este proyecto, ya que no solo permite definir los parámetros necesarios para el correcto diseño del sistema, sino que también dispone dichos parámetros para su futura consulta.

Con dichos parámetros se procede a la selección de los componentes de una manera definida, es decir, no solo influyen estos parámetros, sino que la selección de unos componentes influye sobre los demás. Así, por ejemplo, la selección del accionamiento electromecánico se realiza en función del par resistivo de la puerta, pero sus parámetros de funcionamiento, tensión, potencia y energía consumida influirán de manera decisiva sobre el resto de componentes. Se hace en este caso necesario el trazado de un orden de diseño preciso que permita la selección de componentes de manera unívoca, evitando incompatibilidades o ineficiencias.

Una vez seleccionados los componentes se procede al diseño y fabricación de las diferentes placas de prototipado, considerando las conexiones y los modos de operación que serán necesarios para el correcto funcionamiento del sistema. Se fabrican dos placas, una de ellas encargada de elevar la tensión de la batería y de ejecutar el programa de apertura y cierre y, la otra, encargada de disponer la batería y el sistema de almacenamiento de clave para la correcta autenticación.

El diseño de estas placas se realiza de manera doble, ya que su operación es la que permite analizar los errores del diseño y, por tanto, facilita la mejora del sistema. Por ello, una vez analizado el funcionamiento del prototipo, se procede a la fabricación de un prototipo definitivo. Este prototipo consiste únicamente en la mejora de la tarjeta llave, facilitando la comunicación con la placa principal. Para lograr esta mejora, se procede a la fabricación mediante impresión 3D de un soporte para la introducción de la tarjeta. La conexión se produce mediante contacto superficial entre distintas superficies conductoras presentes en la parte superior de la placa llave y unos perfiles inclinados, provistos de cobre conductor en el interior del soporte.

El funcionamiento del sistema depende directamente de la programación del microprocesador situado en la placa principal. Esta programación es una parte importante del presente proyecto, y su mejora y verificación resultan fundamentales de cara a una operación satisfactoria del sistema. No obstante, con este programa no se pretende la operación de una cerradura en



condiciones reales, sino la demostración de las posibilidades del sistema, así como la verificación del diseño y, en general, de todo el trabajo realizado. Este programa es mejorable de manera intencionada, ya que la programación de un sistema definitivo es un tema de gran amplitud cuyo desarrollo se debería abordar en un trabajo específico.

- **Palabras clave**

- Cerradura electrónica
- Circuito impreso
- Accionamiento Electromecánico

- **Códigos UNESCO**

- 2203.01 Electrónica – Circuitos
- 2203.07 Electrónica – Circuitos integrados
- 3307.03 Tecnología electrónica – Diseño de circuitos

---

---

## ÍNDICE

DEDICATORIA .....	3
Agradecimientos.....	5
Resumen .....	7
• Palabras clave .....	9
• Códigos UNESCO.....	9
Índice .....	11
1 Introducción .....	15
2 Metodología .....	23
3 Estudio de viabilidad.....	27
3.1. Tecnologías existentes.....	27
3.2. Accionamientos .....	28
3.2.1. Cerraduras estilo pomo.....	28
3.2.2. Cerraduras con llave de respaldo .....	29
3.2.3. Bombines de autenticación electrónica .....	30
3.2.4. Smart locks.....	30
3.3. Situación del mercado .....	31
3.3.1. Posibles mercados .....	32
3.4. Problemática.....	33
3.4.1. Sistemas mecánicos.....	33
3.4.2. Sistemas electrónicos .....	34
3.5. Justificación de la línea de desarrollo .....	34
4 Dimensionamiento global .....	39
4.1. Dimensionamiento global .....	39
4.2. Dimensionamiento del prototipo .....	42
5 Diseño PCB placa principal .....	49
5.1. Pre-diseño .....	49
5.1.1. Selección de componentes .....	49
6 PWM .....	59
6.1. Especificaciones .....	59
6.2. Selección de la forma de onda.....	60
6.3. Programación de registros.....	60
7 Diseño de la llave. Interfaz TWI .....	67
7.1. Diseño del prototipo .....	67
7.2. Comunicación TWI.....	68
7.2.1. Fundamentos y operación del componente .....	69

7.2.2. Programación .....	73
7.2.3. Diseño prototipo funcional.....	76
8 Conclusiones y valoración .....	83
8.1. Conclusiones .....	83
8.2. Valoración de impactos .....	84
9 Líneas futuras .....	87
9.1. Innovaciones en la autenticación.....	87
9.2. Automatización y gestión remota.....	89
10 Planificación temporal y presupuesto .....	93
11 Referencias .....	99
12 Anexos.....	103
12.1. Accionamientos .....	103
12.2. Esquema de conexión placa principal .....	104
12.3. Esquema conexión placa llave .....	105
12.4. Diseño PCBs .....	106
12.5. Tareas del proyecto.....	107
12.6. Diagrama de Gantt .....	108
12.7. Bill Of Materials.....	109
Índice de figuras .....	111
Índice de tablas.....	113
Índice de cuadros.....	115
Abreviaturas, Unidades y Acrónimos.....	117
Glosario .....	121

# **1. INTRODUCCIÓN Y ESTADO DE LA TÉCNICA**



## 1 INTRODUCCIÓN

Desde siempre las personas han sentido la necesidad de protegerse y actuar de manera eficaz contra cualquier amenaza para sí mismos o su círculo de confianza. Para lograrlo, es fundamental poseer una ventaja que permita sortear, esquivar o incluso enfrentar la amenaza. A lo largo de la historia de la humanidad, esta sencilla realidad se ha hecho palpable en cualquier ser vivo y, por ende, en las relaciones humanas.

Resulta muy interesante ver como esta manera de obtener una ventaja sobre la amenaza se representa muy claramente en el mundo animal. Por ejemplo, los erizos se protegen de las amenazas, pero no huyen, sino que extienden su coraza de espinas para evitar que otro animal pueda hacerles daño. Es un claro ejemplo de cómo una habilidad específica, en este caso protectora, se desarrolla para conferir una ventaja y permitir así la supervivencia.

Por otro lado, es sencillo hablar de un animal como el toro, aún presente en muchas festividades en España y, por tanto, probablemente conocido por la mayoría de la población de este país. El toro posee una fuerza descomunal a la vez que unos cuernos afilados que le confieren una ventaja en cualquier enfrentamiento. Por ello, el toro enfrenta las amenazas, y las combate.

Un último ejemplo de comportamiento típico en el mundo animal, puede ser la gacela, el ciervo, y otros animales capaces de alcanzar grandes velocidades. Estos seres muestran un claro ejemplo de una habilidad que se ha desarrollado con el fin de proporcionar la capacidad de esquivar y huir de los problemas.

Esta realidad que, como se ha visto, se hace palpable en el mundo animal, también lo es, y más si cabe, en la especie humana. Desde que surgieron los primeros *homo*, hace unos 2,5 millones de años, capaces de tallar la piedra para conseguir instrumentos específicos, la especie ha evolucionado desarrollando una impresionante capacidad para crear tecnología que le permita obtener esa ansiada ventaja sobre el entorno, aunque no siempre con el fin de protegerse. De esta manera, se evidencia como a través del conocimiento y la innovación el ser humano ha sido capaz de obtener lo que otros animales han logrado mediante una evolución fisiológica.

No obstante, como sucede en cualquier otra especie, muchas veces los peligros no provienen del exterior. Este hecho justifica que el desarrollo nunca se haya estancado, sino que se ha convertido en algo necesario para proteger a las personas de sus semejantes. Además, cobra importancia el valor de otras motivaciones, más allá de la propia supervivencia, como actualmente son las ideas o en otro tiempo fue el orgullo, el estatus, o cualquier otra concepción humana.

Esta evolución que, como resulta evidente, ha acabado modificando la escala de valores de las personas, también ha llevado a que el desarrollo no tenga como fin último la propia supervivencia.

Durante los últimos dos milenios se tiene absoluta constancia del desarrollo armamentístico que ha experimentado la raza humana y cómo las continuas innovaciones y últimas tecnologías decantaban la balanza a favor de uno u otro bando. Esto no es de extrañar, ni supone una diferencia respecto a cualquier otra especie, si tenemos en cuenta la capacidad creadora del ser humano. Lo que sí supone una diferencia es el desarrollo que han sufrido industrias como la farmacéutica, los mercados bursátiles o, en general, cualquier eslabón de lo que resulta hoy en día nuestra sociedad y que poco tienen que ver con el hecho de sobrevivir, aunque sigue habiendo un fuerte desarrollo en este sentido.

Desde hace décadas y cada vez en mayor medida, la innovación se enfoca en la prevención y en la protección y, no solo a nivel público, sino que también gran parte de la inversión privada ha apostado por el desarrollo de sistemas de protección y armamento no letal, buscando asegurar la supervivencia con mecanismos que permitan defenderse del ataque o prevenirlo, en lugar de enfrentarlo.

Aunque pueda parecer que se trata de una evolución reciente, realmente no lo es, pues ya hace más de 500 años de la vida de Da Vinci, un inventor con gran difusión mediática, cuyos inventos no tenían, en general, una motivación vital, sino que en muchos casos simplemente buscaba la comodidad o incluso el entretenimiento.

Inventos como la bicicleta, cuya autoría no se puede atribuir de manera unívoca a Da Vinci pero, sin embargo, data de esa época, muestran cómo la innovación no siempre tenía un objetivo vital. En este caso lo que se pretendía era facilitar el transporte, reduciendo el gasto energético a la vez que se optimizaba el tiempo.

A nivel público, cabe destacar las nuevas estrategias militares basadas en la “guerra electrónica”, la proliferación de sistemas de “escudos anti-misiles”, satélites de espionaje e información, sistemas de defensa para vehículos móviles, uso de vehículos no tripulados, etc. También en el terreno de la seguridad, aunque ahora a nivel civil, cabe destacar los enormes presupuestos destinados a inteligencia, para anticiparse a posibles ataques de cualquier índole, o prevención de cualquier tipo, desde accidentes de tráfico hasta violencia doméstica.

El concepto de guerra electrónica resulta bastante representativo a la hora de entender este giro importante de la innovación. Mediante el uso de los últimos sistemas electrónicos y tecnológicos, se pretende determinar, explotar, reducir o impedir el uso hostil de cualquier espectro de energía por parte de un posible enemigo y, a la vez, conservar la capacidad de utilizar dicho espectro en beneficio propio. Esta filosofía evidencia de manera muy clara cómo se pretende aprovechar los recursos de manera óptima con el fin de reducir el enfrentamiento a la mínima expresión, generando una victoria o un sometimiento del atacante, incluso, antes de que se produzca el ataque. [1]

A nivel privado, resulta importante destacar el enorme presupuesto que se destina a la prevención de riesgos, no solo a nivel laboral, sino de todo tipo. Cada vez se invierte más en prevenir pérdidas, desarrollando los sistemas necesarios para evitar en la medida de lo posible



que esas pérdidas ocurran.

Este es el motivo fundamental que lleva a que cada vez se invierta más en desarrollar tecnologías de prevención y protección, que permitan evitar o reducir en la medida de lo posible cualquier tipo de contingencia. El interés para ello no se reduce al que puedan tener aquellas personas que se vean directamente afectadas, sino a toda la cadena de personas que se ven unidas por relación mercantil a aquella.

Entendido lo anterior, ahora resulta evidente la creciente inversión que se destina en particular al desarrollo de sistemas de protección físicos, tanto para domicilios como oficinas, almacenes o recintos de alta seguridad. Resulta indispensable disponer de la tecnología necesaria para proteger los espacios y controlar su uso y acceso.

Como consecuencia de esta necesidad, la innovación humana se ha centrado en su desarrollo desde hace siglos. De hecho, las primeras cerraduras se atribuyen a los egipcios, hace más de 4000 años. El sistema que emplearon era muy similar al actual de tambor de pines, donde un pasador con diferentes muescas deslizaba a través de una abertura, posicionando a la altura adecuada una serie de bulones que se encontraban en el interior. De esta manera se desbloqueaba la puerta y se permitía su apertura. Este mismo sistema se encontró en China en la misma época, por lo que su invención bien pudo ocurrir en otro país.

Posteriormente, en el siglo VI, Teodoro de Samos, originario de la isla de Samos, desarrolló por cuenta propia, y sin haber tenido contacto previo con las antiguas cerraduras egipcias o chinas, un sistema muy similar. Esta cerradura es la más antigua que se conserva y supuso un salto cualitativo en cuanto a la forma y materiales empleados. Estaba fabricada en metal, a diferencia de las anteriores, fabricadas en madera.

Después de que Teodoro inventase la cerradura, esta se expandió por toda Grecia, siendo utilizada posteriormente por otras sociedades, como la romana. Sin embargo, no fue hasta mucho tiempo después, en el siglo XVIII, cuando se empezaron a mejorar los mecanismos, así como a crear normas que permitieran clasificar y estandarizar los distintos tipos de cerraduras.

A mediados del siglo XIX destacó un cerrajero norteamericano, llamado Alfred Hobbs, que desarrolló una cerradura considerada imposible de forzar. Además del desarrollo de este sistema, consiguió vulnerar los mejores sistemas ingleses en la “Gran exhibición de 1851”, empezando así una carrera por desarrollar la cerradura perfecta. Él mismo formó parte de esta carrera, fundando su propia marca “Hobbs Hart & Co. Ltd”.

En el mismo siglo y continente convivió Linus Yale, Ingeniero Mecánico y fabricante, ampliamente conocido por la invención de la cerradura de cilindro, desarrollando la primera cerradura con un sistema de pines como los que se utilizan en la actualidad. Quizá la mayor muestra de su éxito sea la presencia de la marca Yale, a día de hoy, como uno de los principales fabricantes de cerraduras en todo el mundo.

La empresa fue fundada en 1868 con el nombre de “*Yale Lock Manufacturing Co.*” en Stamford (Connecticut) haciéndose cargo de las patentes registradas por Linus Yale Jr. en materia de sistemas de seguridad. Estas incluían, aparte del famoso cilindro, cerraduras de banco, de caja fuerte, de perno y candado. Desde entonces ha continuado innovando extendiéndose al mercado anglosajón, donde se convirtió en el principal empleador de *Willenhall*.

A pesar de mantenerse siempre como uno de los principales fabricantes de cerraduras del mercado, la tarea no ha sido sencilla dada la dura competencia del sector. Los constantes desarrollos y mecanismos que se han venido desarrollando han promocionado la creación de nuevos competidores.

Así en el año 2000 la empresa era adquirida por Assa Abloy. Esta fue fundada en 1994 a partir de las dos empresas que le dan nombre y, tras la adquisición de más de 150 empresas, se ha convertido en la actualidad en el principal fabricante a nivel mundial por volumen de ventas. Entre todas las empresas que conforman a día de hoy el grupo, cabe destacar algunas muy prestigiosas como Chubb, Mul-T-Lock, HID, Lockwood, Securitron y, por supuesto, Yale.

Tanto Assa como Abloy eran empresas suecas con tecnología propia que tuvieron gran éxito y durante su historia exportaron sus sistemas por todo el mundo. Si bien el sistema de Assa presentaba mayor similitud con el ya mencionado sistema de pines patentado por Yale, el mecanismo empleado por Abloy era totalmente distinto, presentando un mayor nivel de seguridad.

Emil Henriksson fue el inventor de la cerradura por bloqueo de tambor de disco, “*disc tumbler lock*” en su idioma natal. Este sistema, empleado por Abloy, consistía en una serie de discos de retención giratorios ranurados que debían alinearse para permitirse encajar sobre una barra lateral. De esta manera se liberaba la cerradura franqueando el acceso. La novedad principal consistía en la ausencia de muelles, lo que los hacía mucho más convenientes para condiciones duras, así como para utilizar en el exterior.

Además de esta particular ventaja de operación presentan una mayor seguridad, debido a la mayor dificultad que presentan para abrir mediante ganzado. Además, resulta imposible el uso de otras técnicas de apertura como es el *bumping*, razón que justifica porque en la actualidad este tipo de cerradura se comercializa como de alta seguridad, aunque no evite la apertura por otros métodos.

Se puede apreciar, por tanto, el gran desarrollo que han experimentado los sistemas de seguridad a través del crecimiento de las principales marcas del sector. Su historia muestra una fuerte competencia cuya baza principal es la innovación, gracias a la cual se explica el éxito de unas u otras. La innovación no solo ha permitido alcanzar mayores niveles de seguridad, sino que ha incentivado a otras empresas a desarrollar otros productos, alcanzando la situación actual.

En la actualidad existen todo tipo de sistemas y mecanismos mecánicos para cualquier situación. No obstante, esta innovación también se ha producido en todos los mercados, lo que

incluye también a los sistemas de intrusión. Por ello, actualmente existen numerosos mecanismos para la apertura de cerraduras mediante diferentes técnicas, los cuales consiguen anular la seguridad en cuestión de minutos.

Se consigue así un mercado diferenciado principalmente por la calidad de los productos, con sistemas más asequibles, pero con un nivel inferior de seguridad, que acaban resultando vulnerables a ciertos ataques, y sistemas más caros, con una calidad superior y, por supuesto, un mayor nivel de resistencia a los ataques, aunque finalmente ninguno de ellos sea invulnerable.

Por otro lado, se ha producido un fuerte desarrollo de la electrónica, aunque no con el objetivo de incrementar el nivel de seguridad sino, más bien, de añadir características adicionales. Un claro ejemplo de esta tendencia se puede apreciar en los sistemas de control de accesos, totalmente extendidos en la actualidad en el ámbito empresarial. Estos sistemas que permiten monitorizar y controlar el movimiento de personas, a veces se utilizan en combinación con otros sistemas más sofisticados como pueden ser aquellos de reconocimiento de imagen u otro tipo de sensores.

Resulta interesante, sin embargo, la aparente apatía demostrada hacia los sistemas electrónicos como medio de autenticación, en lugar de constituir un simple registro de accesos. Más aún, cuando la concepción social de los sistemas electrónicos como aquellos de alta seguridad es totalmente palpable.

Es una escena habitual en muchas películas, así como en todo tipo de realizaciones culturales, aquella en la que se presenta un espacio de alta seguridad, conseguida mediante la última tecnología, resultando ser esta un compendio de diferentes sistemas de autenticación electrónica, como pueden ser sensores biométricos, tarjetas de identificación mediante radiofrecuencia, etc.

Se trata, por tanto, de una realidad el hecho de que la gente concibe los sistemas electrónicos como aquellos que pueden aportar mayor seguridad y, sin embargo, la implantación a nivel doméstico e incluso industrial, es prácticamente nula. Si bien es cierto que existen soluciones avanzadas para determinadas instituciones que requieren altos niveles de seguridad, el coste asociado sigue siendo muy elevado, debido principalmente, a su escasa implantación.

Para lograr la implantación de los sistemas electrónicos a gran escala resulta imprescindible la innovación y el desarrollo que facilite su entrada en mercados muy establecidos. Por ello, es necesario un producto muy elaborado, que presente una curva de aprendizaje muy pequeña o incluso nula y con un coste similar a los sistemas mecánicos que se pretende sustituir.

En esta línea se desarrolla el presente trabajo, con el ambicioso objetivo de desarrollar una infraestructura básica sobre la cual poder construir un complejo sistema de autenticación electrónica.



## **2. METODOLOGÍA Y OBJETIVOS**



## 2 METODOLOGÍA

Como ya se ha comentado, es fundamental el desarrollo de una solución particularmente bien implementada para poder entrar en un mercado muy bien establecido, donde las barreras de entrada son prácticamente culturales. Si bien existe una concepción muy arraigada de las cerraduras electrónicas que hace que sean vistas como sistemas de alta seguridad, lo cual es muy positivo, también existe una desconfianza palpable por todo lo electrónico, en general, debido, principalmente, a la abundancia de productos de baja calidad.

Para lograr entrar en un mercado de estas características se requiere un producto con una calidad muy elevada, a un precio competitivo, de manera que el consumidor pueda verlo como un equivalente a los sistemas convencionales mecánicos. Pero, a la vez, es fundamental que el nivel de seguridad aportado por el sistema sea claramente superior a un sistema mecánico.

La consecución de estas características requiere de un diseño particular, enfocado a resolver estos problemas con exactitud antes de aportar otras mejoras, pero dejando la posibilidad de su incorporación posterior. Esto es realmente importante pues no tendría sentido un sistema electrónico que no fuera capaz de sacar partido al potencial de un buen software.

En este sentido se ha desarrollado el presente proyecto, buscando sentar una base sobre la cual poder implementar posteriormente otras soluciones que completen sus características. De esta manera, el proyecto pretende establecer una idea que se convierta en un punto de inflexión respecto a soluciones alternativas.

Esta idea, como se demostrará a lo largo de este trabajo, permite solucionar los principales inconvenientes que venían presentando los sistemas electrónicos actuales, si bien no todos. Por esta misma razón, se hace hincapié en la condición de proyecto base.

Una vez sentada esta base, será menester la implementación de nuevas funcionalidades y mejoras que completen sus características, llegando a la posición de otras cerraduras electrónicas del mercado, como pueden ser aquellas dotadas de sistemas de comunicación por radiofrecuencia y automatización, pero salvando aquellos inconvenientes que las separan de establecerse como la opción preferida.

De esta manera resultará obvia la adopción de sistemas de comunicación mediante cifrado punto a punto, transmisión de datos por radiofrecuencia, implementación de automatismos orientados a aumentar la comodidad, etc. Todas estas características serán implantables sobre la base que se pretende desarrollar.

La metodología empleada será, por tanto, aquella que facilite en mayor grado la evolución posterior del sistema. No interesa desarrollar características que exijan a futuros investigadores desandar lo andado, empleando tiempo adicional en eliminarlas para poder implantar su solución particular. Se procede pues a seleccionar aquellos protocolos más abiertos, haciendo

uso de los sistemas más básicos, pero atendiendo con profundidad al correcto funcionamiento de la cerradura.

Siguiendo esta línea, se procede a implementar puertos de desarrollo que permitan el acceso directo a todos los terminales, no solo con el objetivo de facilitar la verificación del programa, sino de cara a la fabricación de un prototipo sobre el cual se puedan probar módulos adicionales con nuevas funcionalidades.

En definitiva, el presente proyecto tiene como objetivo desarrollar una cerradura electrónica básica, implementando los sistemas más genéricos, permitiendo una mayor compatibilidad de cara a facilitar el desarrollo futuro de aplicaciones. Además, se profundizará particularmente en dos aspectos, como son la alimentación eléctrica y el mecanismo de apertura, pero sin dejar de lado toda la electrónica de control necesaria para el correcto funcionamiento del prototipo.

A lo largo del presente trabajo, se abordarán los diferentes aspectos de la programación que se han desarrollado y, se explicarán con detalle tanto para ofrecer una referencia rigurosa para entender el sistema, como para facilitar futuras modificaciones. Por otro lado, se ha realizado un profundo estudio mecánico para entender los requerimientos de potencia y par, lo cual es fundamental a la hora de poder seleccionar un accionamiento adecuado.

El estudio mecánico es particularmente importante para el proyecto, dada la metodología aquí explicada, de cara a poder actuar de manera adecuada sobre el sistema de cierre de cada puerta. La diversidad de sistemas de cierre, junto con la necesidad de conformar un producto destinado a un mercado muy amplio, otorgan a este estudio la importancia mencionada y justifican también el hecho de haber realizado las estimaciones muy al alza, dejando amplios factores de seguridad.

Por último, el estudio energético adquiere también una importancia particular, resultado de los requerimientos específicos del accionamiento y de la batería. Dado el uso particular que se le va a dar y, buscando la mayor comodidad posible, se pretende que la batería tenga un factor de forma muy reducido, lo cual reduce la variedad disponible en el mercado. Además, para la consecución efectiva del proyecto resulta fundamental disponer de un balance energético positivo, en cuanto a la diferencia de energía entre lo que consume el accionamiento y lo que dispone la batería.



### **3. ESTUDIO DE VIABILIDAD**



### 3 ESTUDIO DE VIABILIDAD

#### 3.1. Tecnologías existentes

En lo que respecta a los sistemas de seguridad física para el control de accesos, actualmente se pueden encontrar diferentes tecnologías conviviendo. Por un lado, sistemas puramente mecánicos, resultado de la evolución natural de las primeras cerraduras y, por otro, sistemas puramente electrónicos o híbridos, con dos partes distinguibles y diferenciables, una electrónica y otra mecánica.

Los sistemas puramente físicos consisten en bombines o cilindros, candados, cierres corredera y, en general, cualquier tipo de cerradura basada en un mecanismo. El funcionamiento de un bombín se basa en un cilindro trabado por una serie de pistones, cada uno de ellos con una longitud característica y diferente de cualquier otro. Mediante la inserción de la llave se logran alinear los pistones, quedando de esta manera el cilindro liberado.



*Fig. 1: Sección de un cilindro mecánico de 6 pistones. Se puede apreciar el alineamiento de los pistones que desbloquea el cilindro.  
(Fuente: UAP TradeLocks)*

Con el desarrollo de la electrónica surgen diferentes planteamientos de cerradura que buscan prescindir de la llave, bien por incrementar la seguridad (bancos, reservas de seguridad), bien por necesidades particulares (control de accesos) o bien por ambas (por ejemplo, hoteles). De esta manera, salen al mercado las primeras cerraduras en emplear sistemas electrónicos como medio de autenticación.

En la actualidad, existen diferentes sistemas de seguridad basados en autenticación electrónica, manteniendo un accionamiento doble: uno puramente mecánico y otro electromecánico. Obviando el sistema de autenticación empleado, el cual escapa del alcance de este trabajo, sí procede estudiar y valorar la tecnología presente en estos accionamientos, así como el nivel de implantación que logran alcanzar dentro del mercado.

### **3.2. Accionamientos**

El accionamiento empleado de manera mayoritaria, tanto en la industria como en el ámbito doméstico, consiste en el bloqueo del resbalón. Este bloqueo se puede efectuar tanto en el marco de la puerta, propio de accesos a portales comunitarios y sitios donde se requiera un nivel de seguridad bajo, como en la propia puerta, muy empleado en hoteles. Ambos sistemas ofrecen un nivel de seguridad muy bajo ya que no permiten el bloqueo de la puerta mediante el paletón o los bulones, limitándose a liberar el resbalón.

El sistema integrado en el marco presenta la ventaja de no necesitar un diseño específico de la puerta, el cual requeriría que la puerta estuviese cableada. No obstante, este sistema no limita las posibilidades de apertura, sino que ofrece una alternativa adicional para desbloquear el resbalón. Es un caso común que este sistema se acompañe de una puerta con cerradura incorporada, como puede ser un bombín convencional de llave, lo que permite su apertura por dos métodos alternativos: bien desbloqueando mediante el accionamiento electromecánico el anclaje del marco donde encaja el resbalón o, bien, mediante el accionamiento de la llave que retraería el resbalón. Este sistema ofrece dos posibilidades de apertura pero, a cambio, una seguridad baja.

En cuanto al sistema integrado en puerta, se destaca sobre todo en hoteles de medianas y grandes cadenas que cuentan con un sistema de gestión centralizado. Esta tecnología resulta rentable dada la gran cantidad de habitaciones que disponen, aunque en la actualidad con el auge de la electrónica en todos los ámbitos y la particular caída de precios que ha experimentado, se comienza a ver incluso en pequeñas cadenas hoteleras. El principal inconveniente es el coste asociado a la instalación: requiere de puertas adaptadas y un cableado de control y alimentación desde el sistema central hasta cada acceso, o un mantenimiento intensivo en el caso de aquellos sistemas dotados de baterías. No obstante, este no es el único inconveniente, ni el más significativo, ya que la escasa seguridad que ofrece ha sido razón principal de que esta tecnología no se haya exportado a otros ámbitos.

Por otro lado, con un mercado más minoritario y, sobre todo, de ámbito doméstico, se vienen desarrollando sistemas de autenticación electrónica capaces de instalarse en cualquier puerta. Esto lo consiguen mediante unas medidas estándar, ajustadas al perfil del país en cuestión, ya que presentan la forma y dimensiones de un bombín convencional. Dentro de este grupo se pueden distinguir a su vez distintas implementaciones.

#### **3.2.1. Cerraduras estilo pomo**

Estas cerraduras permiten desbloquearse únicamente mediante tecnología RFID. Se pueden combinar con el sistema convencional de bombín, accediéndose tanto con llave mecánica, como con llave electrónica. Para su funcionamiento cuenta en su interior con un grupo de baterías, que proporcionan a la cerradura la energía necesaria para autenticar la llave electrónica y desbloquear la cerradura. En caso de que las baterías se queden sin carga, es posible desmontar la cerradura desde el exterior e introducir unas baterías cargadas.



*Fig. 2: Cerradura electrónica con formato de cilindro estandarizado  
(Fuente: Onity United Technologies)*

Cabe destacar la flexibilidad que ofrecen estas cerraduras, superando a los bombines convencionales. La gran facilidad de instalación unida a las características que ofrecen las posibilidades de control mediante sistemas inalámbricos, automatización, creación de llaves electrónicas virtuales, etc., hacen de este sistema una estupenda alternativa para centros residenciales ubicados en zonas donde la seguridad no sea un problema. Esto se debe al diseño particular de la cerradura, ubicando la alimentación y parte de la electrónica en el lado exterior, lo que compromete sensiblemente la seguridad.



*Fig. 3: Cerradura electrónica con doble sistema de apertura,  
mecánico y electrónico  
(Fuente: Yale Locks)*

### **3.2.2. Cerraduras con llave de respaldo**

Existen sistemas que ofrecen una mayor protección contra vandalismo o posibles intentos de sabotaje, disponiendo las baterías en el lado interior. Para resolver las situaciones de baja carga en las baterías cuentan con dos sistemas: por un lado, se produce un aviso previo cuando el nivel de batería se encuentre bajo un cierto umbral, permitiendo al usuario su sustitución de manera cómoda y, por otro lado, mantienen el bombín tradicional, permitiendo así abrir la puerta en cualquier momento utilizando la llave.

Se trata de una solución conservadora, recomendable para zonas más inseguras que las anteriores, pero siempre teniendo en cuenta las carencias que presenta la cerradura mecánica, lo que hará de este sistema una mera expansión de la cerradura convencional. Gracias a esta implementación resulta posible disfrutar de las bondades que ofrece la electrónica en cuanto a control y automatización, pero no resuelve el problema de inseguridad intrínseco a los sistemas mecánicos. De este problema se hará un estudio en mayor profundidad en el apartado 3.4.1.

### 3.2.3. Bombines de autenticación electrónica

Estos sistemas presentan el nivel más elevado de seguridad, disponiendo un doble sistema de autenticación: además del tradicional sistema mecánico de seguridad, requieren de una verificación electrónica. Para ello la cerradura o la propia llave llevan unas baterías incorporadas. Estas proporcionan al sistema la energía necesaria para que se produzca la autenticación. No obstante, el accionamiento se produce de manera manual por el operador, el cual debe girar la llave para poder desbloquear la cerradura.



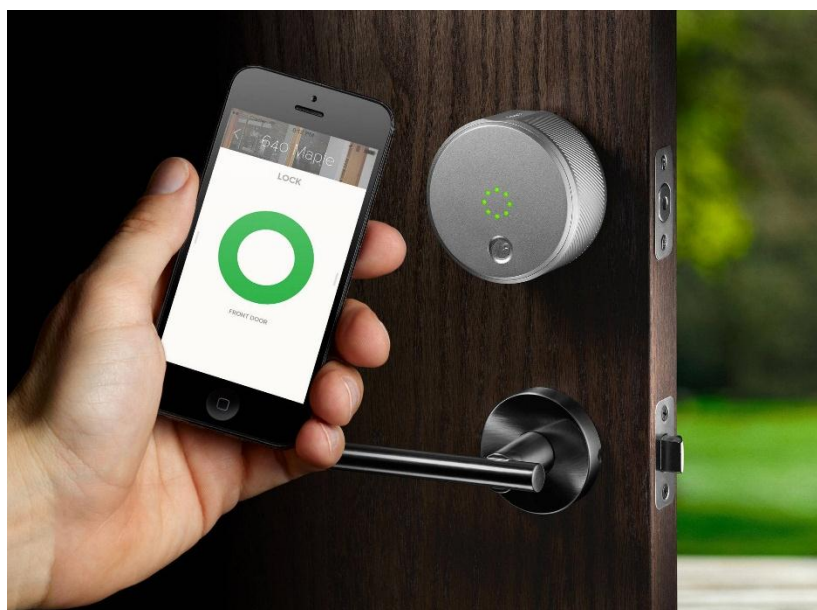
*Fig. 4: Cilindro de seguridad con autenticación electrónica  
(Fuente: Winkhaus blueChip)*

Es muy relevante el nivel de seguridad que ofrecen estos sistemas en la autenticación, convirtiéndose con toda probabilidad en los mejores del mercado en cuanto a posibilidad de descifrado, o apertura sin fuerza. No obstante, aunque solucionan el principal problema de seguridad propio de los cilindros mecánicos, el *bumping* o la apertura mediante ganzuado, no solucionan el segundo y no por ello menos importante: la apertura mediante extractor. Si bien es cierto que dado el diseño de estas cerraduras se dificulta en cierta medida el taladrado del bombín, indispensable para usar el extractor, también lo es que no acaban de evitarlo y, por tanto, supone una brecha de seguridad que puede no compensar el sobreprecio de la cerradura.

### 3.2.4. Smart locks

Se basan en la utilidad que ofrecen las aplicaciones móviles, las cuales permiten la monitorización avanzada del sistema y, muchas veces, en tiempo real. Para ello disponen de

baterías integradas y conexión directa a la red eléctrica, además de una conectividad avanzada (RFID/NFC, WIFI, BLUETOOTH, etc.). Para asegurar el bloqueo de la puerta montan su propio bulón, accionado por un motor integrado en la propia cerradura.



*Fig. 5: Cerradura electrónica “inteligente” con bulón motorizado  
(Fuente: August Smart Lock)*

Estos sistemas son los que han pretendido liderar la verdadera revolución a nivel doméstico ya que, aun disponiendo de un equipo bastante limitado, sobre todo en cuanto a seguridad, ofrecen un entorno de conectividad y gestión muy completo, así como un desarrollo software potente que permite una monitorización extensa y un control íntegro. A pesar de esto, presenta unas carencias de seguridad muy grandes que lo descartan para cualquier entorno en el que no exista otro sistema de seguridad principal.

### **3.3. Situación del mercado**

Cada una de estas tecnologías ocupa una posición dentro del mercado en función de sus características intrínsecas, que las vuelven más o menos favorables para uno u otro uso. Según el estudio realizado queda en evidencia la ausencia de sistemas que aúnen seguridad y posibilidades de control en un mismo dispositivo, aun tratándose de las dos características más fundamentales de cualquier cerradura moderna. La razón de esto se debe principalmente a la focalización del mercado en diferentes segmentos de población, los cuales, a día de hoy, son más receptivos a la actualización de su sistema de seguridad.

En este punto resulta fundamental destacar la importancia que ejerce la cultura sobre las posibilidades de éxito de cualquier iniciativa de este tipo. En la actualidad, la gente tiene una relación casi diaria con sistemas electrónicos de todo tipo, desde la tostadora, el microondas, o la radio, hasta sistemas digitales como “*SMART TV*”, móviles *inteligentes*, o el PC; este aumento exponencial de los sistemas electrónicos ha venido acompañado del desarrollo de todo

tipo de herramientas de intrusión y espionaje, así como la manipulación de objetos cotidianos con el fin de añadirles una funcionalidad de espionaje que no se menciona al usuario. Este es el caso de los móviles que se comercializan, preparados de fábrica o en un proceso posterior, o de las herramientas de software que emplean tanto gobiernos como empresas privadas para acceder a equipos privados [2]. Tanto las filtraciones que han salido a la luz en los últimos tiempos, como la inseguridad que provoca el uso de sistemas informáticos (PCs, tabletas, etc.) por temor a robos de información, suplantación de identidad, infección de malware y demás delitos informáticos, genera en gran parte de la población una desconfianza generalizada a la seguridad de cualquier sistema electrónico.

Cabe destacar también el efecto psicológico que tiene el uso de sistemas mecánicos, dando al usuario una sensación de falsa seguridad: mientras que en una cerradura convencional es común pensar que dejando la llave por el interior resultará imposible abrirla desde el otro lado, ya que la leva queda bloqueada, en la cerradura electrónica no se dispone de un mecanismo que garantice visualmente al usuario que la cerradura está bloqueada.

### **3.3.1. Posibles mercados**

Después de analizar la situación actual del mercado resulta evidente la concentración de sistemas electrónicos en torno a dos conceptos distintos pero muy bien definidos. Por un lado, se encontrarían las cerraduras enfocadas a mejorar la seguridad, añadiendo sistemas adicionales de autenticación electrónica y, por otro, se encontrarían aquellos sistemas cuyo objetivo es simplemente aumentar las funcionalidades de las cerraduras convencionales, aunque ello suponga una disminución de la seguridad. Por tanto, se vuelve evidente la ausencia de un sistema que combine las dos características anteriores, incorporando un avanzado software de control que permita exprimir al máximo las funcionalidades potenciales de la puerta, pero a la vez, mejorando la seguridad con la última tecnología de cifrado disponible.

A continuación, se abordan algunos mercados, enumerando las ventajas que podrían resultar de interés para los potenciales clientes:

- Entornos de baja seguridad:

Serían aquellas residencias situadas en barrios tranquilos o que ya cuentan con algún tipo de seguridad en el recinto, lo que vuelve innecesario la instalación de puertas de seguridad. En esta situación, la seguridad adicional que aporta la cerradura electrónica es inútil, pues el punto débil se encontraría en la propia puerta, en lugar de en la cerradura. No obstante, sigue aportando grandes ventajas para estos entornos ya que añadiría funcionalidades interesantes como el control de accesos, mayor seguridad en los accesos comunitarios, puertas inteligentes con apertura asociada al pago de una tasa, etc.

- Entornos de seguridad media:

Referido a aquellas zonas cuyo acceso debe ser protegido de manera eficaz, pero cuya vulneración no corre gran riesgo. En este grupo se podrían englobar aquellas zonas de



acceso restringido ubicadas en lugares públicos, donde resulta de gran interés disponer de un control sobre los accesos, pero a la vez, disponiendo sistemas de elevada seguridad que impidan el acceso de personas no autorizadas.

También se encontrarían en este grupo aquellas viviendas situadas en barrios seguros, pero cuya seguridad depende únicamente de este sistema y, por tanto, resulta importante asegurar su fiabilidad. Otro caso importante dentro de este mismo grupo serían los vehículos, los cuales siguen incorporando una cerradura mecánica que permita la apertura en caso de que se agote la batería. En este caso, aunque la seguridad en la autenticación no se pueda mejorar, ya que la mayoría dispone de autenticación electrónica con cifrado de alto nivel sí que se podría eliminar la cerradura mecánica, lo cual es el mayor punto vulnerable en la actualidad.

- Entornos de alta seguridad:

Referido a aquellos contextos donde la seguridad es un factor fundamental. Es el caso de industrias y otras corporaciones con grandes intereses en proteger equipos, información y/o espacios, viviendas situadas en barrios conflictivos o donde la seguridad cobre un papel fundamental, así como en embajadas y edificios de alto interés que puedan ser objetivo de actos delictivos. En todas estas circunstancias se vuelve realmente interesante disponer de un sistema que garantice los niveles de seguridad más altos, a la vez que provee funcionalidades de control avanzadas.

### **3.4. Problemática**

#### **3.4.1. Sistemas mecánicos**

La sencillez de un sistema mecánico que, si bien ha permitido durante muchos años garantizar una relativa seguridad a un coste reducido, también se ha mostrado como una debilidad en los últimos tiempos. La proliferación de dispositivos mecánicos y electromecánicos que permiten a cualquier persona abrir una cerradura de este tipo supone una amenaza para la seguridad de todas las personas y de las instituciones. Mejorar la seguridad de las cerraduras a un precio asequible que permita su uso a la mayoría de la población resulta indispensable para asegurar el progreso de la sociedad.

El principal problema de estos sistemas es la falta de seguridad debido a la innovación en los sistemas de intrusión. El desarrollo de mecanismos específicos para la apertura forzada vuelve a los sistemas mecánicos vulnerables. A parte del clásico ganzuado, el cual requiere cierta técnica para poder llevarlo a cabo, existen otros métodos como el “bumping” o la extracción.

El “bumping”, técnica también conocida con el nombre de “ramping” consiste en la apertura de cilindros mecánicos mediante la percusión de los pistones, gracias a llaves específicamente diseñadas para esta tarea. Al introducir esta llave en una cerradura y golpearla con un martillo, la energía se transmite de la llave a los pistones, pero como estos se encuentran bloqueados por la llave, la energía se transmite de estos a los contrapistones, los cuales se desplazan sobrepasando la línea de corte durante un breve instante, suficiente para desbloquear la

cerradura. Actualmente, las cerraduras mecánicas de alta seguridad incluyen diseños específicos para dificultar el uso de esta técnica, aunque no acaban de evitarla por completo. [2]

La extracción es un método mucho más invasivo que el anterior, ya que busca romper el cilindro para desplazar los bulones de la puerta de manera manual. Para ello se taladra el cilindro y se introduce un tornillo de suficiente sección. A continuación, mediante un dispositivo específico anclado a la puerta, se procede a tirar del tornillo, provocando la rotura del cilindro por la parte central. [3]

### **3.4.2. Sistemas electrónicos**

Los sistemas electrónicos que se comercializan en la actualidad no acaban de desarrollar una alternativa completamente autónoma, dependiendo en muchos casos de cerraduras mecánicas, bien por ofrecer un sistema adicional en caso de error o fallo del suministro eléctrico, o bien por la desconfianza del usuario ante la posibilidad de no poder desbloquear el acceso. Debido a que no acaban de prescindir de los sistemas mecánicos, presentan las mismas debilidades que estos.

Las cerraduras electrónicas que se comercializan en la actualidad cuentan con cifrados de alta seguridad, con algoritmos que se han demostrado seguros hasta la fecha en muchas otras aplicaciones.

### **3.5. Justificación de la línea de desarrollo**

Tras el análisis de la situación actual resulta evidente la necesidad de sustituir aquellos sistemas críticos que empleen una comprobación puramente mecánica para autorizar el acceso, dada su limitada seguridad, aunque sí se puede conservar dicho sistema como una comprobación auxiliar, necesaria pero no suficiente. En su lugar se utilizará un sistema de autenticación puramente electrónico. El presente proyecto pretende desarrollar la base para poder implementar cualquier sistema de autenticación electrónico sobre una cerradura común, evitando la dependencia de un sistema de autenticación mecánico, palpable en todos los productos que se encuentran actualmente en el mercado.

El principal inconveniente de prescindir del bombín o cilindro mecánico, a la vez que se implementa un sistema de autenticación electrónico, es la alimentación del sistema. Se deben prever situaciones como fallos de alimentación o altos costes de instalación eléctrica que dificultan o imposibilitan la conexión del sistema a la red eléctrica. Soluciones basadas en baterías también albergan un riesgo por la posibilidad de descarga, y una incomodidad asociada al mantenimiento periódico. La solución adoptada para resolver dichos inconvenientes pasa por albergar la energía del sistema en la propia llave. De esta manera, la llave no solo se encarga de presentar un mecanismo de autenticación, sino que almacena la energía y la dispone al sistema para permitir su operación.

Dejando de lado las posibles soluciones que se puedan desarrollar en un momento puntual para resolver problemas particulares, y que no se deban a verdaderas carencias del sistema, resulta evidente que el mencionado contexto de inseguridad informática supone una gran barrera para la implantación de una cerradura completamente electrónica resultando de gran importancia abordar dicho problema de manera previa al desarrollo de un sistema completamente comercial. No obstante, dado el alcance de este trabajo, es especialmente interesante trasladar dicho problema a líneas futuras que pretendan la implantación real de los sistemas que se abordan. Por ello, se ha decidido posponer el problema desarrollando un módulo completamente aislado, siendo el lector para la llave-tarjeta la única conexión posible con la cerradura y, por tanto, el único punto vulnerable. Esta decisión no anula las posibilidades de gestión remota y monitorización, sino que se trasladan a una fase de diseño posterior, centrando el presente trabajo en el funcionamiento mecánico y eléctrico de la cerradura, así como en la interfaz tarjeta-cerradura.

Aunque se desarrollará con profundidad en el capítulo 0, cabe destacar la enorme flexibilidad que ofrece esta solución, como una razón añadida para su elección, no solo en lo referente al protocolo de autenticación, sino también en el sistema de alimentación y la posibilidad de monitorización y control remoto. Gracias al amplio abanico de soluciones existentes, tanto inalámbricas (RFID, NFC, WiFi, Bluetooth...) como cableadas, se abre la posibilidad de ampliación y mejora del sistema, tanto en nivel de seguridad ofrecida como en prestaciones y servicios.

Aunque el análisis de viabilidad técnica y el dimensionamiento se podrían haber desarrollado en el presente estudio de viabilidad, se ha preferido dedicar un capítulo íntegro a este aspecto dada la relevancia que tendrá sobre el resto del trabajo.



## **4. DIMENSIONAMIENTO MECÁNICO**



## 4 DIMENSIONAMIENTO GLOBAL

El desarrollo de un accionamiento electromecánico que permita controlar una cerradura diseñada para operar de manera manual requiere de un dimensionamiento preciso, no solo del par motor requerido por el accionamiento, sino también de la potencia necesaria. Estas dimensiones varían en gran medida en función del mecanismo considerado (n.º de bulones, profundidad de anclaje de los bulones, complejidad del mecanismo, etc.), así como del estado en que se encuentre (óxido, deformaciones debido al calor o golpes, etc.), y ello puede provocar un funcionamiento incorrecto e incluso el bloqueo permanente del acceso.

### 4.1. Dimensionamiento global

Como parte del dimensionamiento se comienza analizando una cerradura interna de una puerta de acceso a vivienda. Se ha seleccionado un caso muy desfavorable, tratándose de una puerta con 20 años de antigüedad y cierres mediante bulones a lo largo de todo el canto de la puerta. Para llevar a cabo las mediciones del par requerido se procede a diseñar un mecanismo que permita medir el par aplicado a la llave durante el proceso de cierre.

El mecanismo elegido consiste en un eje de diámetro definido,  $d$ , unido de manera solidaria a la llave. Este eje lleva enrollado un cable, al final del cual se dispondrá un recipiente. Será preciso tener en cuenta la masa del recipiente, pero no la del cable, el cual se desprecia debido a su pequeña densidad y longitud. Se introduce la llave en la cerradura y se marca el ángulo inicial. A continuación, se vierte un fluido de densidad conocida,  $\rho$ , en el recipiente, y simultáneamente se anota el ángulo girado por la llave en función del volumen de líquido que se halle en el recipiente.

Este método presenta la desventaja de que la fuerza ejercida solo puede aumentar o mantenerse, en función de si vertemos más líquido o no, respectivamente, mientras que resulta imposible retirar fluido y, por tanto, también lo es medir un par inferior al ya alcanzado. No obstante, ofrece la posibilidad de medir el valor máximo, lo cual es suficiente para seleccionar el accionamiento a emplear.

La **¡Error! No se encuentra el origen de la referencia.** permite obtener el par a partir de la fuerza ejercida sobre el cable, resultado del peso conjunto del recipiente,  $R$ , más el fluido,  $\rho \cdot V$ , y del radio del eje.

$$M = (P + \rho \cdot V) \cdot g \cdot R$$

*Ecuación 41*

Siendo  $M$  el par y  $V$  el volumen de fluido vertido en el recipiente. Los datos recogidos, se muestran en la Tabla 1, y el valor del par en la Ecuación 42.

Ángulo	Tiempo (s)	Par (N·m)	Potencia (W)	Energía (J)
0	0,00	0,00	0,00	0,00
10	0,06	0,00	0,00	0,00
20	0,11	0,00	0,00	0,00
30	0,17	0,00	0,00	0,00
40	0,22	0,00	0,00	0,00
50	0,28	0,00	0,00	0,00
60	0,33	0,00	0,00	0,00
70	0,39	0,00	0,00	0,00
80	0,44	0,00	0,00	0,00
90	0,50	0,00	0,00	0,00
100	0,56	0,00	0,00	0,00
110	0,61	0,00	0,00	0,00
120	0,67	0,00	0,00	0,00
130	0,72	0,00	0,00	0,00
140	0,78	0,00	0,00	0,00
150	0,83	0,00	0,00	0,00
160	0,89	0,00	0,00	0,00
170	0,94	0,00	0,00	0,00
180	1,00	0,19	0,61	0,03
190	1,06	0,19	0,61	0,07
200	1,11	0,19	0,61	0,10
210	1,17	0,19	0,61	0,14
220	1,22	0,19	0,61	0,17
230	1,28	0,19	0,61	0,20
240	1,33	0,19	0,61	0,24
250	1,39	0,19	0,61	0,27
260	1,44	0,00	0,00	0,27
270	1,50	0,00	0,00	0,27
280	1,56	0,00	0,00	0,27
290	1,61	0,00	0,00	0,27
300	1,67	0,00	0,00	0,27
310	1,72	0,00	0,00	0,27
320	1,78	0,00	0,00	0,27
330	1,83	0,00	0,00	0,27
340	1,89	0,00	0,00	0,27
350	1,94	0,00	0,00	0,27
360	2,00	0,00	0,00	0,27

*Tabla 1: Valores medido de par de apertura de una cerradura instalada en una puerta doméstica convencional.  
(Fuente: Elaboración propia)*

$$M = (30 + 1000 \cdot 0,5) \cdot 9,8 \cdot 0,033 \cdot 10E - 3 = 0,19404N \cdot m$$

*Ecuación 42*



Este par es perfectamente alcanzable por un gran número de motores DC de tamaño reducido, con tensiones de funcionamiento bajas (5 – 12V), lo que reduce los costes al no ser necesario el diseño de un componente a medida. Al contrario, la amplitud de mercado provoca precios reducidos, por tratarse de especificaciones muy demandadas. Por tanto, queda probada la viabilidad a nivel mecánico, aunque no eléctrico, ya que la potencia disponible para efectuar tanto la apertura como el cierre es limitada.

Para el cálculo de la potencia requerida será preciso determinar la velocidad de apertura/cierre, que determinará junto con el par, según la Ecuación 43, dicha potencia. Es obvio que la velocidad de accionamiento es una variable que forma parte del diseño, y como tal, su elección dependerá de las condiciones de funcionamiento que se deseen.

$$P = M \cdot \omega$$

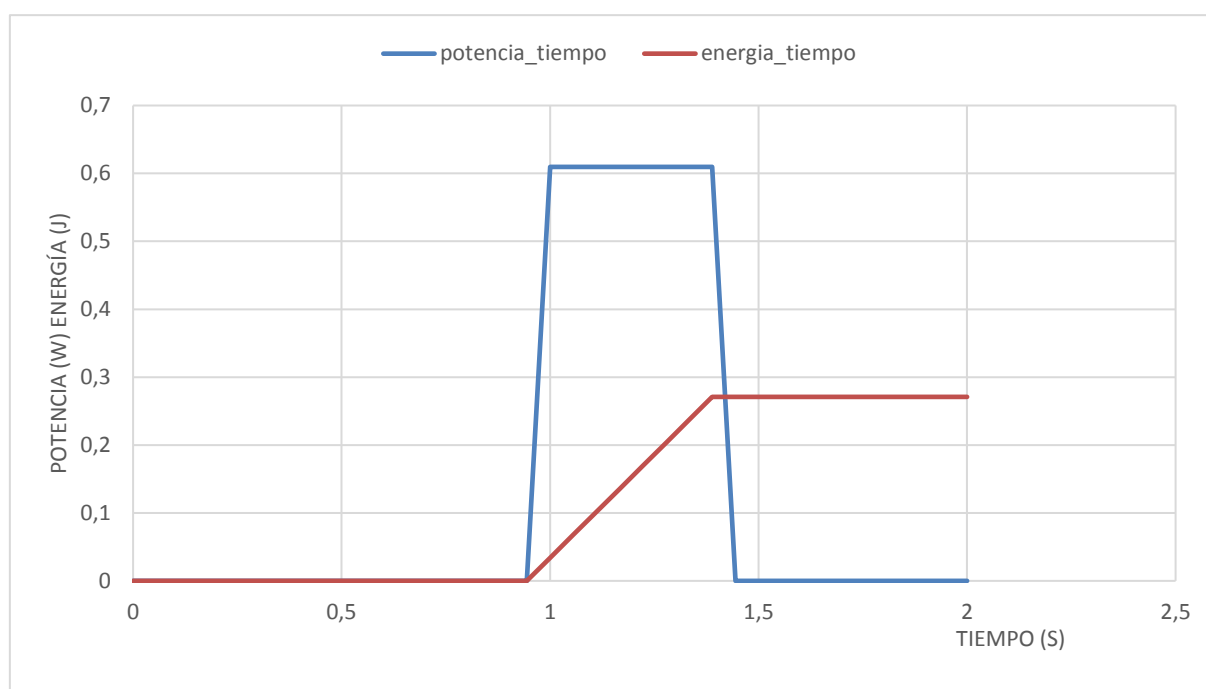
*Ecuación 43*

Para determinar la velocidad se considera adecuado esperar hasta 6 segundos a que el mecanismo se bloquee/desbloquee. Dado que el mecanismo requiere 3 vueltas completas en uno u otro sentido en función de la acción a realizar, esto supone 2 segundos por vuelta, o lo que es lo mismo, aproximadamente 30RPM. Si se tiene en cuenta el valor del par máximo hallado con anterioridad, y según la Ecuación 44 se puede obtener la potencia máxima requerida.

$$P_{MAX} = 0.19404N \cdot m \cdot \pi rad/s = 0.6096W$$

*Ecuación 44*

Esta potencia hace referencia al valor máximo que alcanza y que, por tanto, deberá suministrar la fuente de alimentación en el momento preciso. No obstante, durante la mayor parte del movimiento el accionamiento se encuentra girando en vacío, ofreciendo un par resistente prácticamente nulo, lo que hace que la potencia sea también nula. Debido a lo anterior será preciso tener en cuenta el par resistente ofrecido en función del ángulo girado para poder hallar la energía empleada. Estos datos resultan difíciles de obtener, como ya se ha comentado, debido al método empleado para medir el par. Aun así, se puede realizar una aproximación al alza verificando de manera manual los ángulos en los cuales el par resistente es nulo y considerando el resto como de par resistente máximo. Esta aproximación provoca una onda cuadrada en una gráfica potencia-ángulo, cuya integración devuelve el valor de la energía buscado, si se tiene en cuenta la dependencia entre el ángulo y el tiempo. La energía representada se refiere al área abarcada por la función potencia hasta el instante de tiempo considerado.



*Gráfico 1: Potencia y energía requerida para la apertura de una cerradura a velocidad constante en función del tiempo.  
(Fuente: Elaboración propia)*

En la Tabla 1 se detallan los datos medidos, así como la potencia y energía halladas. El valor de la energía resulta ser de 0'27 Julios por vuelta, o lo que es lo mismo, 0'81 Julios por bloqueo/desbloqueo. Por tanto, se requiere una llave que albergue al menos 1 Julio de energía, y que sea capaz de proporcionar una potencia de al menos 0'61W, lo que se traduce en 122mA a 5V o 51mA a 12V. Estos valores no solo son perfectamente asumibles por las baterías más reducidas disponibles en el mercado, sino que además ofrecen unas características mucho más elevadas, permitiendo la operación de varios ciclos de apertura/cierre sin la necesidad de recargar la batería.

Debido al interés y creciente desarrollo que se está produciendo en la actualidad de los sistemas de almacenamiento de energía, cabe la posibilidad de emplear condensadores planos para albergar la carga, permitiendo la fabricación de llaves de tamaño ultrareducido, pero con unas capacidades de carga y descarga prácticamente instantáneas.

## 4.2. Dimensionamiento del prototipo

Como parte del proyecto se ha desarrollado una maqueta que permita recrear las condiciones de operación reales. Esta maqueta consiste en una cerradura a tamaño real dispuesta sobre una puerta de madera en miniatura. Como cerradura se ha seleccionado un modelo de embutir de la marca TESA.

La cerradura seleccionada sería un caso aún más desfavorable que la del caso general. Esta requiere un giro de la llave muy reducido, pero presenta un desplazamiento del bulón en función del ángulo girado mayor, por lo que toda la energía se debe absorber en un giro más reducido, resultando en potencias más elevadas. En particular, el ángulo recorrido por la llave es de 180

grados.



*Fig. 6: Cerradura de embutir marca TESA  
(Fuente: TESA – ASSA ABLOY)*

Para medir el par se vuelve a emplear el método utilizado para el dimensionamiento general, cuyo resultado en este caso es 0'2456 N·m. Comparando con el valor obtenido anteriormente se comprueba que es mayor, en concreto, un 26% mayor. Esto no tiene por qué ser necesariamente así, ya que la interpretación previa permitía intuir una mayor potencia, pero no necesariamente mayor par resistivo.

$$\frac{P_{actual}}{P_{anterior}} \cdot 100 = \frac{0,2456}{0,19404} \cdot 100 = 126 \quad \text{Ecuación 45}$$

A diferencia de como se ha procedido anteriormente, ahora no es conveniente fijar la velocidad del accionamiento de manera arbitraria, sino que dicho valor debe ser extraído de las características del accionamiento elegido. No obstante, si resulta conveniente que dicho valor sea al menos superior a 30RPM, que se corresponde con una vuelta cada dos segundos.

Para la selección del accionamiento se procede a determinar los parámetros que condicionan su elección. En este caso, el primer parámetro limitante es el par, medido en 0,2456 N·m, por lo que consideraremos un par mínimo de 0'25 N·m.

El siguiente factor limitante debe ser la tensión de funcionamiento fijada en 5 Voltios. La razón de fijar este valor para la tensión se debe a la reducción de costes y el aumento de eficiencia del sistema, ya que la tensión que ofrecen la mayoría de baterías es de 3,7 Voltios. Teniendo en cuenta el interés de reducir en la medida de lo posible el tamaño de la llave, no resulta conveniente disponer varias baterías en serie para aumentar la tensión, ya que ello conllevaría un mayor tamaño del dispositivo. Por otro lado, la eficiencia de un elevador de tensión disminuye cuanto mayor es la diferencia entre tensión de entrada y salida. Además, conviene

resaltar la amplitud de mercado en lo que a servomotores se refiere, lo cual permite encontrar con facilidad numerosos accionamientos de distintos fabricantes que satisfacen ambos factores a un precio razonable.

Como último factor técnico se hallaría la velocidad la cual, como ya se ha comentado, no conviene fijar de manera arbitraria, pero sí se debe acotar por motivos de utilidad, pues no resulta cómodo ni práctico un sistema de cierre que tarde demasiado en actuar. Debido a lo anterior se limitará la velocidad de giro a un valor mínimo de 30RPM.

El último y definitorio factor a considerar es el coste.

En la tabla completa de accionamientos situada en el anexo 12.1, se pueden observar los accionamientos formados por un motor eléctrico y un engranaje reductor que cumplen todos los factores anteriores, ordenados de mayor a menor coste. Si bien el precio de los motores es bastante reducido no sucede lo mismo con los engranajes, que pese a proporcionar rendimientos medios tienen un coste muy elevado.

Sin embargo, la combinación de motor y engranaje no es la única solución que se puede adoptar, o por lo menos no lo es adquiriendo dichos elementos por separado. En el mercado se pueden encontrar otro tipo de motores donde el engranaje va integrado en el propio cuerpo del motor, servomotores, que incluyen su propia electrónica de control, la cual permite controlar la velocidad del accionamiento sin necesidad de controlar el flujo de potencia eléctrica al motor, o al menos no de forma directa. Este es el caso del servomotor elegido, de la marca “Parallax”, que ofrece la capacidad de controlarlo mediante PWM a través de una línea sin potencia.

La velocidad máxima ofrecida por este motor es de 50RPM. De acuerdo a la Ecuación 43, la potencia máxima requerida será de 1'286W. Esta potencia se refiere al valor máximo requerido, el cual no se mantiene de manera constante. La cerradura seleccionada dispone de un mecanismo que ofrece un par resistente a partir de cierto ángulo. Esto provoca que al girar dicho ángulo la cerradura acabe de completar el cierre por sí misma. No obstante, si lo que se pretende es abrir, se debe vencer el par resistente desde el comienzo del giro, hasta volver al ángulo mencionado anteriormente. Esta asimetría de funcionamiento provocará una distribución distinta del par en función del movimiento realizado, aunque la energía total debe ser muy parecida, pues al basar su funcionamiento en un resorte este únicamente almacena la energía, siendo las diferencias una consecuencia de los rozamientos del mecanismo. Por tanto, el par resistivo más elevado se dará en el proceso de cierre, mientras que en la apertura aumentará de manera progresiva hasta el ángulo límite, siendo el máximo en cualquier caso inferior al de cierre.

Para la medición del par resistivo en función del ángulo se procede comprobando de manera manual cuando el par es mayor o menor. Este método, aunque impreciso, permite dibujar una curva de par aproximando a valores superiores. Además, gracias a la forma particular de la curva de par, resulta posible medir éste en varios puntos, no únicamente el valor máximo. Todo ello ha permitido elaborar los gráficos Par/Energía-Ángulo representados en la Gráfico 2.

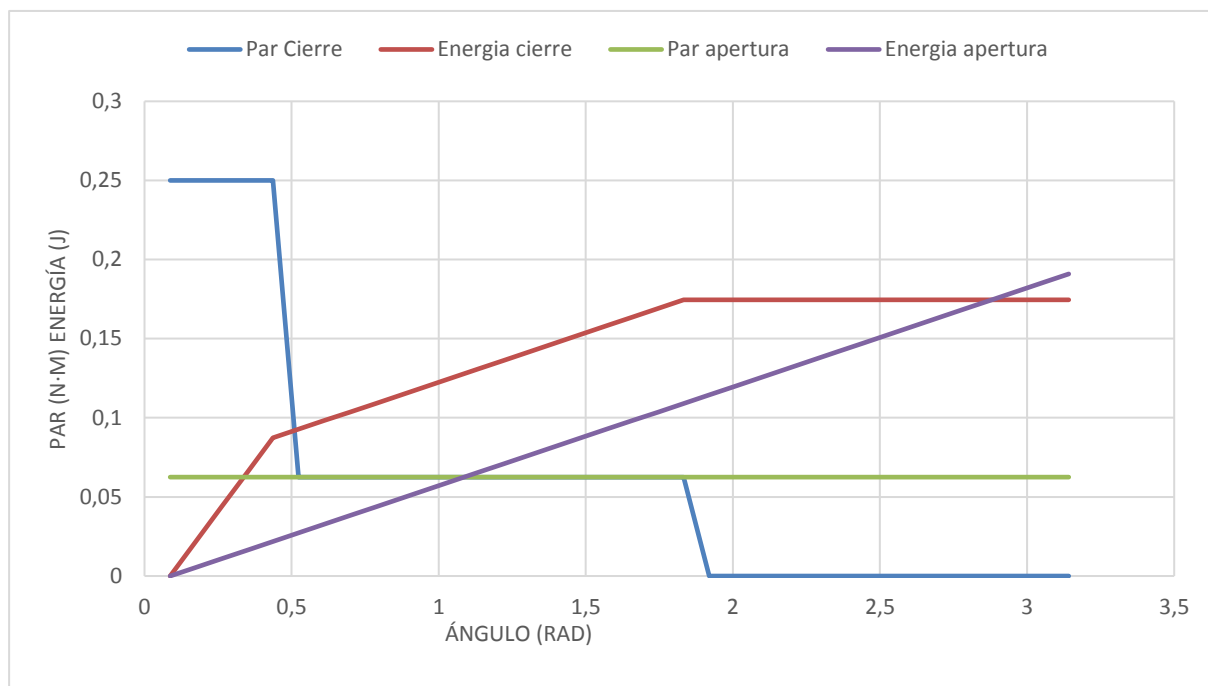


Gráfico 2: Potencias y energías de apertura y cierre en función del ángulo girado por la llave.  
(Fuente. Elaboración propia)

Para obtener el Gráfico 2 se ha procedido mediante integración numérica, según la Ecuación 47 que permite obtener la potencia en función del ángulo girado, dada la relación fija entre ángulo y tiempo a través de la velocidad de giro, parámetro del motor.

$$\dot{\varphi} = \frac{d\varphi}{dt} \quad \text{Ecuación 46}$$

$$\text{Potencia} = M \cdot \omega = M(\varphi) \cdot \dot{\varphi} \quad \text{Ecuación 47}$$

$$\text{Energía} = \int_0^t P \cdot dt = \int_0^t M(\varphi) \cdot \dot{\varphi}(\varphi) \cdot dt = \int_0^\varphi M(\varphi) \cdot d\varphi \quad \text{Ecuación 48}$$

El análisis de esta gráfica muestra como la energía en la apertura es muy parecida, pero superior a la energía empleada en el cierre, a pesar de que el par en la apertura es muy inferior.

Referido al caso límite, aquel en el cual la potencia demandada por el motor es mayor, se producirá en el punto de máximo par, ya que la velocidad de giro del servo se considera constante. En la práctica esta velocidad no es constante, sino que presenta ligeras variaciones mientras se opera dentro del umbral de par permitido, lo que explica las diferencias del valor teórico respecto al real. En la Ecuación 411 se calcula la intensidad teórica que demandará el motor en la situación de máximo par, a partir de las ecuaciones Ecuación 49 y Ecuación 410.

$$P = V \cdot I \quad \text{Ecuación 49}$$

$$P = M(\varphi) \cdot \dot{\varphi} \quad \text{Ecuación 410}$$

$$I = \frac{P}{V} = \frac{M(\varphi) \cdot \dot{\varphi}}{V} = \frac{0,25N \cdot m \cdot 5,236 \text{ rad/s}}{5V} = 0,2618A \quad \text{Ecuación 411}$$

## **5. DISEÑO PCB PLACA PRINCIPAL**





## 5 DISEÑO PCB PLACA PRINCIPAL

La cerradura se acciona mediante un servomotor, el cual se controla mediante una placa PCB. En una primera fase (fase de pre-diseño) se procederá al diseño de una placa PCB de alimentación, capaz de amplificar la tensión de la batería hasta los valores nominales requeridos por el servomotor. Posteriormente, como parte de la misma fase, se desarrolla un primer prototipo compuesto por el circuito de alimentación probado con anterioridad y el microprocesador, así como las salidas convenientes para facilitar la programación del micro y la conexión al dispositivo de identificación. La segunda y última fase de diseño (prototipado) consiste en el desarrollo de un prototipo final y totalmente funcional, siendo este su principal objetivo, aunque sin dejar de lado aspectos como el volumen final del dispositivo, la estética o la facilidad de montaje/desmontaje.

### 5.1. Pre-diseño

#### 5.1.1. Selección de componentes

El desarrollo de la placa de alimentación se articula en torno al componente encargado de elevar la tensión, esto es, un *convertidor boost*. Se trata de una fuente de alimentación conmutada, la cual, mediante la operación de interruptores semiconductores, permite elevar la tensión en continua [4]. Además de los interruptores dispone de condensadores y/o inductores para almacenar energía. También se disponen elementos pasivos para homogeneizar la señal y disminuir el rizado.

Teniendo en cuenta la tensión nominal de trabajo que demanda el servomotor que se va a emplear (5V), seleccionaremos el *convertidor boost* de manera acorde. No obstante, este no es el único parámetro a tener en cuenta, ya que resulta de gran importancia asegurar que la corriente máxima demandada por el circuito no va a superar los valores límites del componente elevador de tensión, aun dejando cierto margen, conveniente para proteger el elevador de tensión de sobrecargas. Esta corriente ya ha sido calculada de manera teórica, y tras las pruebas realizadas sobre el servomotor, también ha sido obtenida de manera experimental, estando ambos resultados detallados en el apartado de dimensionamiento 4.2.

La mencionada intensidad máxima que recorre el circuito se debe principalmente a la potencia requerida por el servomotor, pero no únicamente. A la energía consumida por el motor hay que añadirle las pérdidas debidas al rendimiento del elevador de tensión, así como al consumo del resto de componentes electrónicos, tanto el microprocesador y la memoria, como los componentes pasivos. Por tanto, antes de poder seleccionar el elevador de tensión y la batería, será necesario seleccionar el resto de componentes, teniendo en cuenta la tensión de funcionamiento del motor (5V). En la Fig. 7 se detalla un diagrama simplificado del orden de selección de los componentes.

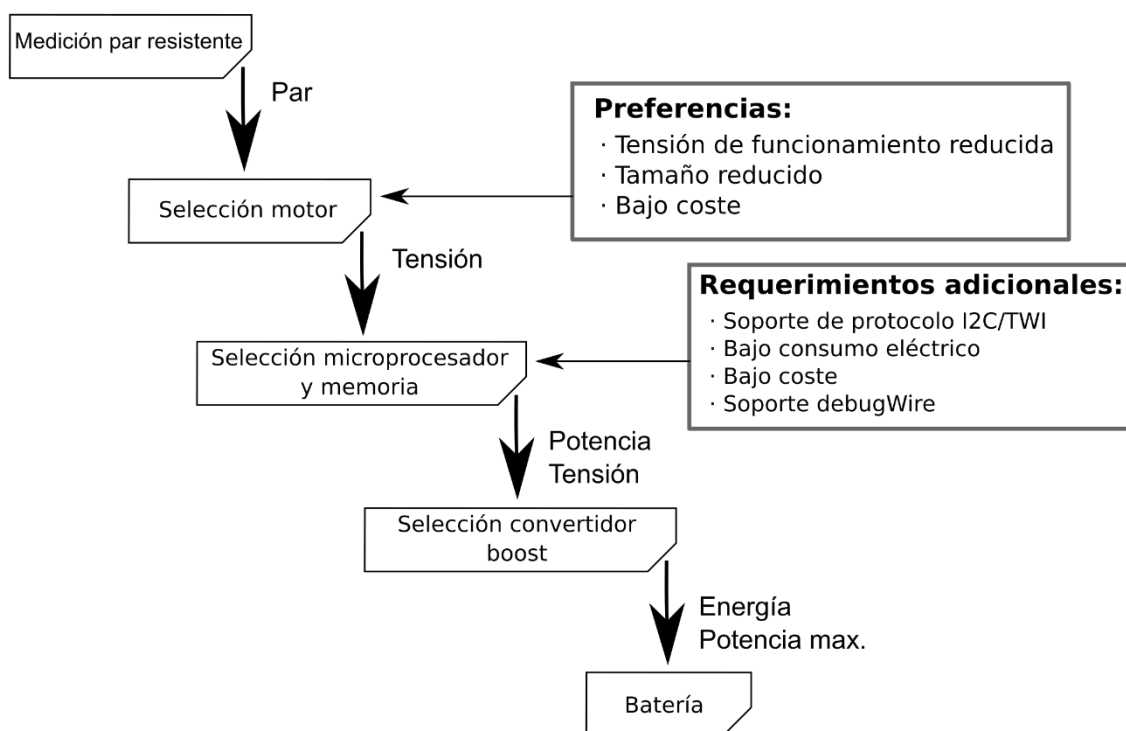


Fig. 7: Diagrama de proceso para selección de componentes  
(Fuente: Elaboración propia)

## Microprocesador

La característica fundamental que debe reunir el microprocesador, la cual permite seleccionar la gama de productos sobre la que escoger el modelo determinado, es el bajo consumo eléctrico, así como la baja potencia de procesamiento. Para este cometido, se ha seleccionado la marca Atmel, en particular la gama tinyAVR [4], optimizada según el propio fabricante, para aplicaciones que requieren rendimiento, eficiencia energética y facilidad de uso. Como dato concreto, cabe destacar la posibilidad de trabajar sobre tensiones muy reducidas, de hasta 0,7 Voltios, lo cual permitiría establecer dos circuitos trabajando a diferente tensión, uno para la electrónica de control trabajando a la tensión de la batería y otro para alimentar el servomotor proporcionando la tensión nominal de este, 5 voltios. Esta modificación permitiría aliviar ligeramente el elevador de tensión, pero sobre todo eliminar el rizado y posible ruido que se genere en caso de un malfuncionamiento del componente.

Además del consumo, otra característica que se ha tenido en cuenta es el soporte para el protocolo I2C mediante hardware. No obstante, aunque un gran número de productos de la gama ofrecen dicho soporte en modo esclavo, no es así en modo maestro, no habiendo ninguno que reúna dicha característica. Esta es la razón que motivará la implementación del soporte I2C mediante software. Además del soporte I2C es importante que el microprocesador sea compatible con la interfaz de depuración debugWire (dW) o similar soportada por la placa *DragonAVR* [5], ya que esta es la tecnología disponible en el departamento.

En cuanto a potencia de procesamiento, pines disponibles y memoria flash todos los modelos superan con creces las necesidades de la aplicación. Cabe mencionar una funcionalidad interesante presente en algunos modelos de la gama, *picoPower*® (pP) [6], que ofrece distintos modos de operación con consumos muy reducidos, permitiendo apagar ciertos sectores del micro en función de las necesidades. En la Tabla 2 se muestra una comparativa de los principales modelos de la gama y algunas de sus características más representativas. Se puede apreciar como cualquiera de estos modelos cumple los requisitos mínimos que se han establecido, por lo que la elección definitiva se realiza en base al coste del componente y a la fecha de comercialización, por temas de soporte, escogiendo finalmente el modelo ATtiny441.

Modelo	Flash (kBy-tes)	Número de pines	Freq. (MHz)	SPI	UART	pP	dW	Tensión
ATtiny25	2	8	20	1	0	No	SI	1.8 a 5.5
ATtiny45	4							
ATtiny85	8							
ATtiny24	2	14	20	1	0	No	SI	1.8 a 5.5
ATtiny44	4							
ATtiny84	8							
ATtiny24A	2	14	20	1	0	Si	SI	1.8 a 5.5
ATtiny44A	4	14	20	1	0	Si	SI	1.8 a 5.5
ATtiny84A	8	14	20	1	0	No	SI	1.8 a 5.5
ATtiny441	4	14	16	1	2	Si	SI	1.7 a 5.5
ATtiny841	8	14	16	1	2	Si	SI	1.7 a 5.5
ATtiny2313	2	20	20	2	1	No	SI	1.8 a 5.5
ATtiny2313A	2	20	20	2	1	Si	SI	1.8 a 5.5
ATtiny26	2	20	16	1	0	No	SI	2.7 a 5.5
ATtiny261A	2	20	20	1	0	Si	SI	1.8 a 5.5
ATtiny4313	4	20	20	2	1	Si	SI	1.8 a 5.5
ATtiny43U	4	20	8	1	0	Si	SI	0.7 a 5.5
ATtiny461	4	20	20	1	0	No	SI	1.8 a 5.5
ATtiny461A	4	20	20	1	0	Si	SI	1.8 a 5.5
ATtiny48	4	32	12	1	0	Si	SI	1.8 a 5.5
ATtiny828	8	32	20	1	1	Si	SI	1.7 a 5.5
ATtiny861	8	20	20	1	0	No	SI	1.8 a 5.5
ATtiny861A	8	20	20	1	0	Si	SI	1.8 a 5.5
ATtiny87	8	20	16	2	1	No	SI	1.8 a 5.5
ATtiny88	8	32	12	1	0	Si	SI	1.8 a 5.5
ATtiny1634	16	20	12		2	Si	SI	1.8 a 5.5
ATtiny167	16	20	16	2	1	No	SI	1.8 a 5.5

Tabla 2: Comparativa procesadores bajo consumo de la marca Atmel  
(Fuente: Elaboración propia a partir de la información facilitada por el fabricante)

Según la hoja técnica del microprocesador elegido, este consume en modo activo 0.2mA funcionando a 1.8 voltios y 1MHz, lo que supone una potencia de 0.36mW.

## Memoria

Una vez seleccionado el microprocesador y teniendo en cuenta la tensión de operación resulta sencillo seleccionar una memoria compatible. Como requisito principal se establece el soporte del protocolo I2C, aunque también es necesario una capacidad superior a 128 bytes para poder establecer una clave de cierta seguridad, aunque en el prototipo inicial se operará con claves de 1 byte. No obstante, este requisito no se aplica en la práctica, ya que todos los modelos ofrecen como mínimo 1024 bytes de capacidad, por lo que se acaba escogiendo el modelo en función del coste. La Tabla 3 muestra una comparativa de las características de algunos modelos de memorias compatibles con el protocolo I2C de la marca Atmel.

Modelo	Tensión	Capacidad	I/O Pins	Tamaño de bloque (Bytes)	Disposición
AT24C01C	1.7 a 5.5	1Kb	5/8	8	128 x 8
AT24C02C	1.7 a 5.5	2Kb	5/8	8	256 x 8
AT24C04C	1.7 a 5.5	4Kb	5/8	16	512 x 8
AT24C08C	1.7 a 5.5	8Kb	5/8	16	1024 x 8
AT24C128C	1.7 a 5.5	128Kb	8	64	16384 x 8
AT24C16C	1.7 a 5.5	16Kb	5/8	16	2048 x 8
AT24C256C	1.7 a 5.5	256Kb	8	64	32768 x 8
AT24C32D	1.7 a 5.5	32Kb	5/8	32	4096 x 8
AT24C512C	1.7 a 3.6 2.5 a 5.5	512Kb	8	128	65536 x 8
AT24C64B	1.8 a 5.5 2.7 a 5.5	64Kb	8	32	8192 x 8
AT24C64D	1.7 a 5.5	64Kb	5/6/8	32	8192 x 8
AT24CM01	1.7 a 5.5	1Mb	8	256	131072 x 8
AT24CM02	1.7 a 5.5	2Mb	6	256	262144 x 8
AT24CS01	1.7 a 5.5	1Kb	5/8	8	128 x 8
AT24CS02	1.7 a 5.5	2Kb	5/8	8	256 x 8
AT24CS04	1.7 a 5.5	4Kb	5/8	16	512 x 8
AT24CS08	1.7 a 5.5	8Kb	5/8	16	1024 x 8
AT24CS16	1.7 a 5.5	16Kb	5/8	16	2048 x 8
AT24CS32	1.7 a 5.5	32Kb	5/8	32	4096 x 8
AT24CS64	1.7 a 5.5	64Kb	8	32	8192 x 8
AT24HC02C	1.7 a 5.5	2Kb	8	8	256 x 8
AT24HC04B	1.8 a 5.5	4Kb	8	16	512 x 8
AT24MAC402	1.7 a 5.5	2Kb	5/8	16	256 x 8
AT24MAC602	1.7 a 5.5	2Kb	5/8	16	256 x 8
AT34C02D	1.7 a 5.5	2Kb	5/8	16	256 x 8
AT34C04	1.7 a 3.6	4Kb	8	16	512K x 8

*Tabla 3: Comparativa memorias flash de bajo consumo de la marca Atmel  
(Fuente: Elaboración propia a partir de la información facilitada por el fabricante)*

Finalmente se escoge el modelo AT24C01C. Estos dispositivos presentan unos consumos máximos durante el proceso de escritura y lectura, siendo este último el que interesa para definir

el consumo máximo. Según la hoja técnica este consumo se sitúa en 1mA operando a 5 voltios y 400KHz, lo que supone 5mW.

## **Elevador de tensión**

Como ya se ha comentado, para la elección de este componente es necesario conocer la potencia consumida por el circuito, por lo que en primer lugar conviene calcular dicho consumo en función de los componentes elegidos, aunque finalmente su influencia sea mínima. Para contrastar el dato, es suficiente con comparar la potencia máxima demandada por el motor, calculada en el apartado correspondiente del dimensionamiento mecánico, de 1,286W, con la potencia requerida de manera continuada por la parte lógica del circuito, microprocesador más memoria, de 5,36 mW.

De esta manera, una vez calculada la potencia, la intensidad soportada por el componente elevador de tensión dependerá de la tensión de funcionamiento, según la Ecuación 49. Esta intensidad, 260mA, hace referencia a una tensión de funcionamiento de 5 Voltios. No obstante, las especificaciones de los dispositivos para elevar la tensión suelen referirse a la intensidad de entrada, por lo que conviene hallar dicha intensidad.

Para hallar la intensidad de entrada hay que tener en cuenta la eficiencia del elevador Ecuación 512, la cual varía en función de la diferencia de tensiones y de la propia intensidad. Debido a esto puede resultar un cálculo de gran complejidad, al no disponer de las funciones reales del rendimiento, sino de gráficas aproximadas proporcionadas por el fabricante. Por ello, se va a proceder mediante un proceso de cálculo iterativo.

$$\eta = \frac{P_s}{P_e} \quad \text{Ecuación 512}$$

Para comenzar se va a suponer un rendimiento efectivo del 70%, cifra bastante inferior a lo habitual. Según la Ecuación 513, y admitiendo que la tensión proporcionada por la batería es constante y de valor 3,7V, se obtiene la intensidad de entrada.

$$I_e = \frac{P_s}{V_e \cdot \eta} = \frac{1,286W}{3,7V \cdot 0,7} = 496mA \quad \text{Ecuación 513}$$

Una vez obtenidos estos datos, se procede a la selección del componente más adecuado. En este caso, simplemente debe verificarse que la tensión de salida es la adecuada y que la intensidad máxima del componente no se supere en ningún caso, dejando, además, cierto margen de seguridad. Una vez cumplidos estos parámetros, se seleccionará el componente en función de su eficiencia y coste, según se puede verificar en la Tabla 4.

<i>Modelo</i>	Tensión de salida (V)	Intensidad máxima de entrada (A)	Tensión mínima de entrada (V)	Eficiencia (a 300mA)	Tamaño	Precio
<i>UIV10F5</i>	5	1.2	0.5	90%	0.35" × 0.45"	4.49
<i>UIV11F5</i>	5	1.2	0.5	87%	0.45" × 0.6"	4.95
<i>U3V12F5</i>	5	1.4	2.5	87%	0.32" × 0.515"	3.95
<i>U3V50F5</i>	5	5	2.9	93%	0.6" × 1.9"	13.95
<i>LTC3529</i>	5	1.5	1.8	95%	8-Lead, 2mm × 3mm	2.93
<i>LTC3125</i>	5.25	1.2	1.6	90%		3.22
<i>LTC3426</i>	5.5	2	1.6	93%		2.14

Tabla 4: Comparativa elevadores de tensión  
(Fuente: Elaboración propia)

Finalmente se escoge el modelo LTC3529, el cual, además de cumplir todas las especificaciones y disponer el rendimiento más elevado, también ofrece el precio más bajo. Este componente requiere su instalación en un circuito impreso junto con una serie de elementos pasivos, con el fin de optimizar su funcionamiento. No obstante, la selección de estos componentes pasivos tiene su objetivo en adecuar las características del componente para el funcionamiento en otros entornos distintos de aquel para el cual ha sido diseñado. Dado que la especificación de diseño coincide con exactitud con el uso que en este proyecto se le va a dar, se emplearán las especificaciones de los componentes pasivos recomendadas por el fabricante [8]. En ellas se puede comprobar el circuito básico requerido para su funcionamiento, junto con el resto de componentes y sus valores de diseño.

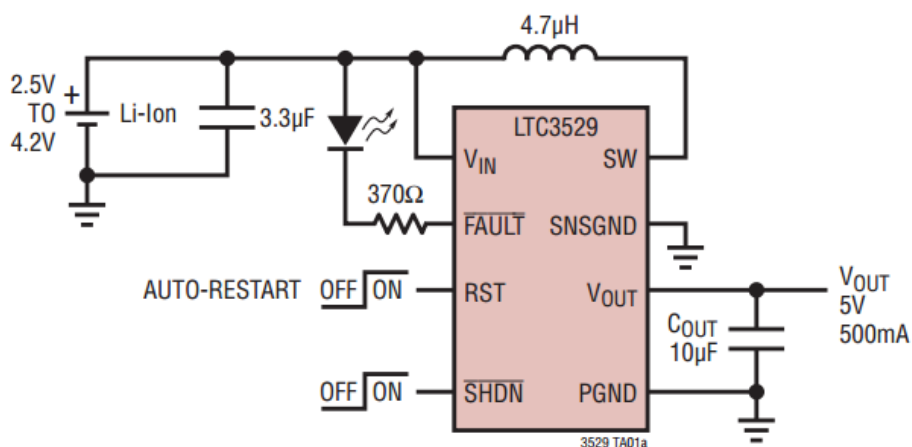


Fig. 8: Diagrama de conexión del componente elevador de tensión LTC3529  
(Fuente: Linear Technology)

## **Batería**

La selección de la batería se puede realizar una vez obtenidos los parámetros anteriores en base a la tensión de funcionamiento y a la tasa de descarga, como valores específicos de diseño pero, además, debe asegurarse que dispone de energía suficiente como para alimentar el sistema un número aceptable de ciclos de funcionamiento.

Si bien la tensión de funcionamiento de las baterías se especifica en voltios, no sucede lo mismo con la tasa de descarga, la cual se suele especificar en función de la capacidad de la batería. De esta manera una batería con una capacidad de 500mAh con una tasa de descarga de 1C, será capaz de descargarse con una intensidad máxima de 500mA. Teniendo en cuenta que la mayoría de baterías disponen de una tasa de descarga mínima de 1C, y que la intensidad máxima demandada por el circuito será de 500mA, debe asegurarse que la capacidad de la batería sea de al menos 500mAh.

Por conveniencia se ha seleccionado una batería estándar de reducidas dimensiones y elevada capacidad, 2500mAh, de la cual se dispone en el departamento. Esta batería dispone una tensión de 3,7V a la salida, lo cual resulta óptimo de cara al elevador de tensión, cuya eficiencia aumenta cuanto menos es la diferencia entre la tensión de entrada y salida.





## **6. PWM**



## 6 PWM

Para el correcto funcionamiento del accionamiento seleccionado resulta necesario adecuar la salida del microcontrolador a los requerimientos de aquel. Para ello, será necesario implementar la técnica de modulación por ancho de pulsos, más conocida por sus siglas en inglés PWM (Power Width Modulation). Esta técnica es ampliamente utilizada hoy en día, no solo para el control de potencia, sino también para transmitir múltiple información a través de un único canal.

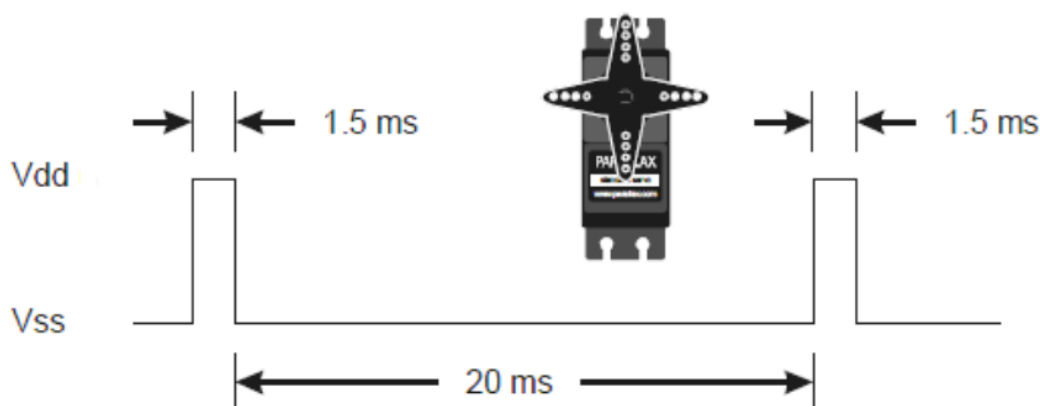
### 6.1. Especificaciones

La hoja técnica del servomotor empleado indica el aspecto que deben presentar los pulsos, así como las características mecánicas en función de dicho aspecto. Dicha hoja establece la anchura de los pulsos en tensión (+Vcc) como regulador del sentido y velocidad de giro proporcionados por el motor, mientras que el espacio entre dichos pulsos debe ser siempre de 20ms. Según esto una anchura de 1,3 ms supone un giro en sentido horario de máxima intensidad, mientras que si el pulso tiene un ancho de 1,7 ms efectuará lo propio en sentido antihorario. Para anchuras de pulsos intermedias entre estos valores se obtendrán, de manera lineal, velocidades de giro también intermedias entre los máximos, 50 RPM en ambos sentidos.

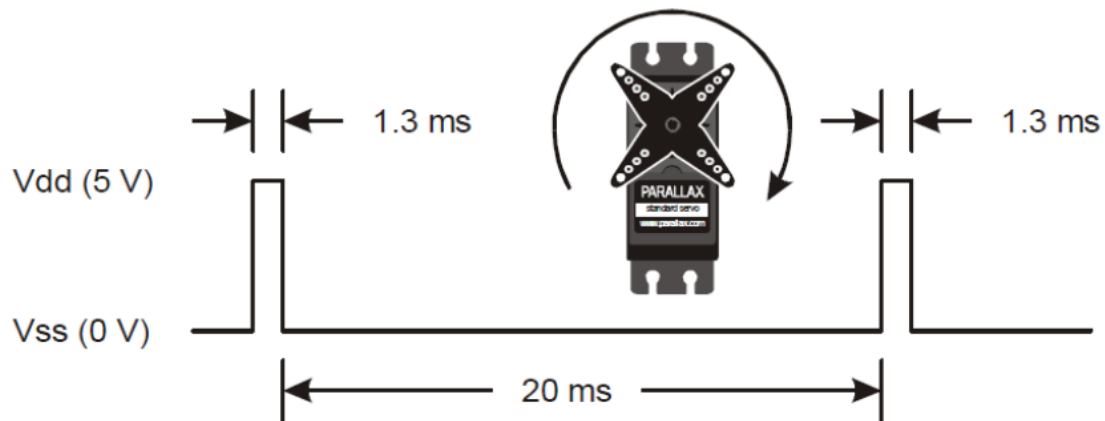
Pin	Name	Description	Minimum	Typical	Maximum	Units
1 (White)	Signal	Input; TTL or CMOS	3.3	5.0	$V_{servo} + 0.2$	V
2 (Red)	$V_{servo}$	Power Supply	4.0	5.0	6.0*	V
3 (Black)	$V_{ss}$	Ground		0		V

*Tabla 5: Especificaciones de tensión para el correcto funcionamiento del servomotor  
(Fuente: Parallax Inc.)*

Para el correcto funcionamiento del servo, será necesario suministrar una tensión de entre 4 y 6 voltios en los bornes de aquel, mientras que el pin de control puede ser accionado mediante una señal de tensión entre 3,3 y 5 voltios, pero siempre menor que la tensión de alimentación del servo más dos décimas.



*Fig. 9: Protocolo de comunicación PWM para operar el servomotor en modo de parada  
(Fuente: Parallax Inc.)*



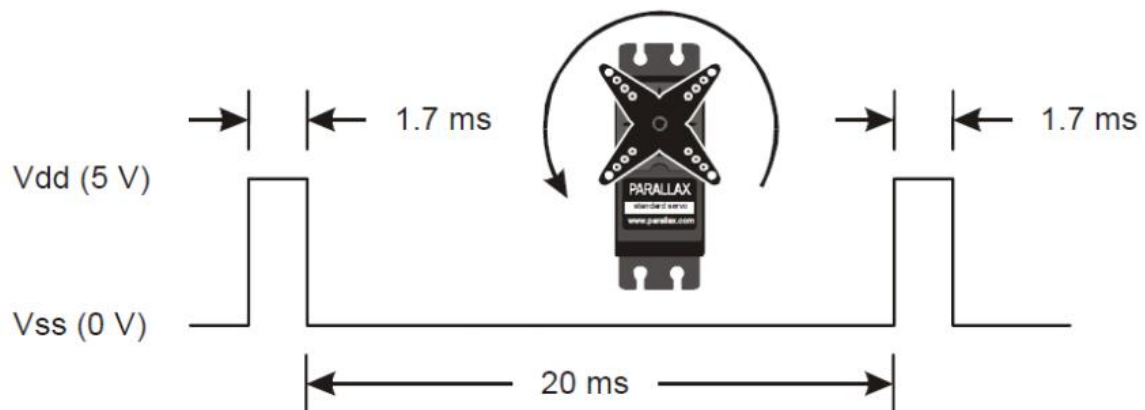
*Fig. 10: Protocolo de comunicación PWM para operar el servomotor a velocidad máxima en sentido horario  
(Fuente: Parallax Inc.)*

## 6.2. Selección de la forma de onda

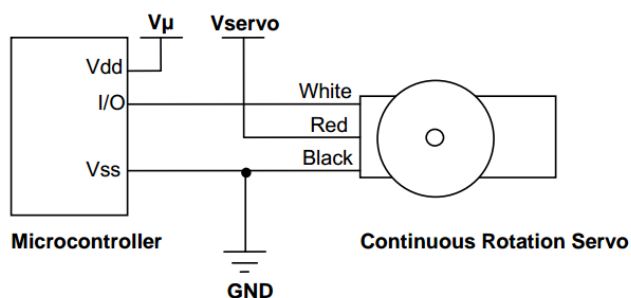
Para el control de los pulsos se hará uso del "timer" incluido en el propio microcontrolador, el cual mediante distintos registros ofrece la posibilidad de gestionar dichos pulsos a través del hardware, evitando así mermar la capacidad de procesamiento, a la vez que asegura un determinado nivel de precisión difícil de alcanzar mediante software.

## 6.3. Programación de registros

Prácticamente la totalidad de los pines del micro nos ofrecen la posibilidad de gestión mediante el timer interno. En particular todos los que llevan la denominación "TOCCn", siendo n el número de pin en cuestión. Una vez seleccionado el pin a utilizar, se comprueba el puerto de comparación de salida asociado (OC – Output Compare pin).



*Fig. 11: Protocolo de comunicación PWM para operar el servomotor a velocidad máxima en sentido antihorario  
(Fuente: Parallax Inc.)*



$V_{\mu}$  = microcontroller voltage supply

$V_{servo}$  = 4 to 6 VDC, regulated or battery

I/O = PWM TTL or CMOS output signal, 3.3 to 5 V;  $< V_{servo} + 0.2$  V

Fig. 12: Diagrama de conexiones del servomotor elegido  
(Fuente: Parallax Inc.)

El control de dichos puertos se efectúa mediante los registros COM (Compare Output Mode). Estos se encuentran para el timer de 16 bit en los registros TCCR1A y TCCR2A. De esta manera, variando el valor de dichos registros se hace posible configurar los puertos de salida en el modo PWM deseado, o devolver el funcionamiento al modo normal.

En cuanto a los modos de operación el microcontrolador *avr* ofrece diferentes configuraciones en función de la forma de onda y de la cuenta realizada en cada ciclo de reloj. Así se incrementa la cuenta del timer en una unidad en cada ciclo, y una vez se alcanza el valor TOP la cuenta se reinicia si está habilitado el modo "FAST PWM" o decrece si se está utilizando el modo "Phase Corrected PWM". Las formas de onda de ambos modos son características e influyen en la duración y precisión de los ciclos.

TOCCn Output	TOCCnS1:0		
	00	01	1X
TOCC0	OC0B	OC1B	OC2B
TOCC1	OC0A	OC1A	OC2A
TOCC2	OC0B	OC1B	OC2B
TOCC3	OC0A	OC1A	OC2A
TOCC4	OC0B	OC1B	OC2B
TOCC5	OC0A	OC1A	OC2A
TOCC6	OC0B	OC1B	OC2B
TOCC7	OC0A	OC1A	OC2A

Tabla 6: Dirección de los registros TOCC  
(Fuente: Atmel Corporation)

El modo escogido para este trabajo ha sido el corregido en fase ya que la cuenta dura el doble de tiempo para el mismo valor TOP. Esto no es algo imprescindible, sino que también se podría haber efectuado con el modo "FAST". No obstante, el modo corregido en fase, como su propio nombre indica, sitúa el centro de los pulsos a distancias constantes, incluso cuando se produce

un cambio en la frecuencia, mientras que en el modo "FAST" sí se varía la posición media de los pulsos al variar la frecuencia de los ciclos. Esto es especialmente útil cuando se requiere

COMnA1 COMnB1	COMnA0 COMnB0	Description
0	0	Normal port operation, OCnA/OCnB disconnected
0	1	WGMn3=0: Normal port operation, OCnA/OCnB disconnected WGMn3=1: Toggle OCnA on Compare Match, OCnB reserved
1	0	Clear OCnA/OCnB on Compare Match when up-counting Set OCnA/OCnB on Compare Match when downcounting
1	1	Set OCnA/OCnB on Compare Match when up-counting Clear OCnA/OCnB on Compare Match when downcounting

Tabla 7: Especificación de los registros COMnAx y COMnBx con modo "Fast PWM" activado  
(Fuente: Atmel Corporation)

una distancia constante entre pulsos, como es el caso que aquí se trata.

El control de los ciclos se efectúa mediante la comparación de dos señales, según muestra el diagrama de bloques. El reloj seleccionado determina la forma de onda que será comparada para obtener los pulsos, ya que en cada ciclo la lógica de control determina la acción a realizar en función del valor del timer, logrando de esta manera satisfacer el modo seleccionado. Así, un valor distinto de la frecuencia del micro proporcionará un incremento más rápido del

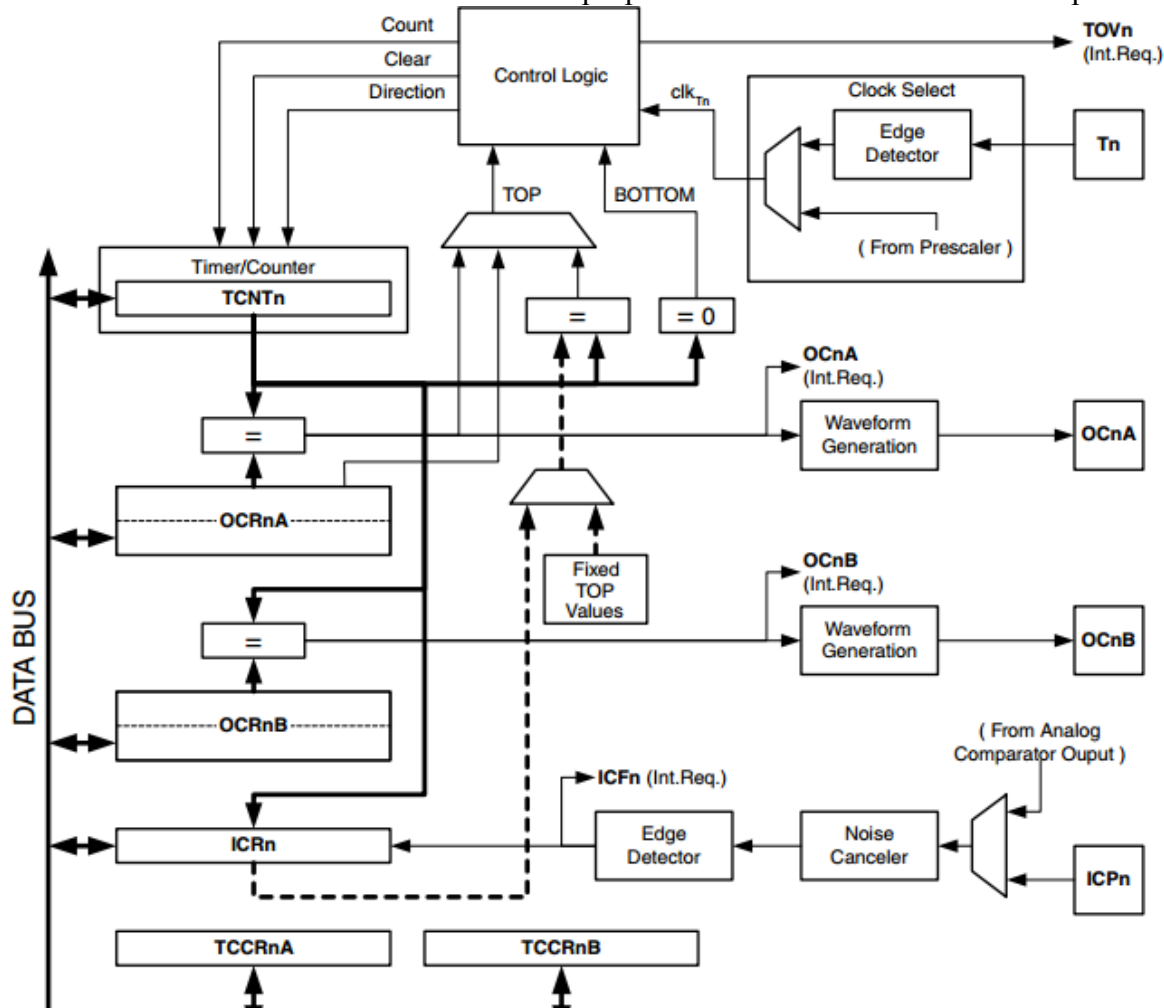


Fig. 13: Diagrama de bloques del "timer" de 8 bits  
(Fuente: Atmel Corporation)

contador y, por tanto, un ancho menor de la forma de onda si la representamos en función del tiempo.

En el control que abarca este trabajo se busca una frecuencia de pulsos tal que la distancia entre ellos sea constante, como ya se ha comentado con anterioridad. Para lograrlo, teniendo en cuenta que vamos a trabajar en modo corregido e invertido en fase, será necesario marcar un valor de comparación ("IC") constante a la vez que variamos el valor TOP. Como se puede apreciar en la Fig. 14 al mantener un valor de comparación constante, la distancia entre los pulsos también lo es, aunque se varíe el valor límite de cuenta.

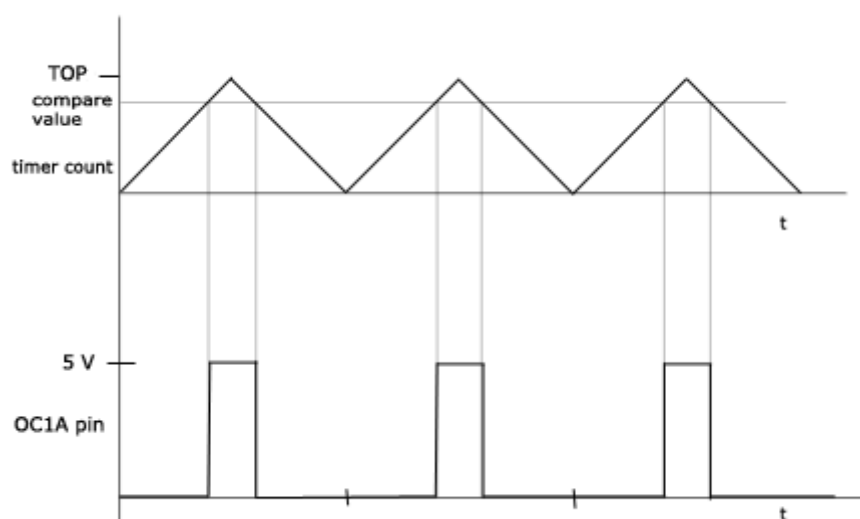


Fig. 14: Diagrama de frecuencias PWM para un valor de comparación constante  
(Fuente: appusajeev blog [9])

Para hallar los diferentes valores de cuenta máxima, así como el valor de comparación, es suficiente con analizar la geometría de la curva. Esto permite deducir dos expresiones cuya solución devolverá los valores buscados.

$$2 \cdot TOP \cdot Periodo = 20 + l \quad \text{Ecuación 14}$$

$$2 \cdot IC \cdot Periodo = 20 \quad \text{Ecuación 15}$$

La primera expresión tiene en cuenta la longitud total de la forma de onda, desde que su valor es 0 hasta que vuelve a serlo, mientras que la segunda solo tiene en cuenta el tiempo entre pulsos, que al ser constante no depende de  $l$ , siendo  $l$  el ancho del pulso elevado. Con este desarrollo es posible obtener una tabla de valores de  $TOP$  para cada velocidad del motor deseada.

$\omega$ (RPM)	I	TOP	CPU freq.	1 MHz
50	1,3	10650	Prescaler	1
37,5	1,35	10675	Periodo	0,001 ms
25	1,4	10700	Periodo low	20 ms
12,5	1,45	10725	IC	10000
0	1,5	10750		
-12,5	1,55	10775		
-25	1,6	10800		
-37,5	1,65	10825		
-50	1,7	10850		

*Tabla 8: Tabla de valores de pico (TOP) en función de la velocidad de giro deseada (izquierda) y tabla de especificaciones necesarias para el cálculo de dichos valores (derecha)*  
(Fuente: Elaboración propia)



## **7. DISEÑO DE LA LLAVE. INTERFAZ TWI**



## 7 DISEÑO DE LA LLAVE. INTERFAZ TWI

El desbloqueo y apertura de la cerradura se realiza una vez se ha comprobado que la llave utilizada tiene autorización. Esta verificación requiere de una conexión y transmisión de información y potencia eléctrica entre cerradura y llave, que se realiza por contacto físico. En este contacto se transmite a la cerradura una corriente continua de 3,8 Voltios proveniente de la batería incluida en la llave. Esta potencia eléctrica alimenta el circuito interno de la cerradura. La cerradura, como parte de su programación, se comunica con la llave de nuevo, transmitiéndole una tensión de 5 Voltios para alimentar la memoria que lleva integrada y permitir así el acceso a la clave contenida en ella. Una vez verificada la clave, se realiza la apertura de la puerta, si procede.

En el presente trabajo se desarrollará un primer prototipo donde la comunicación entre cerradura y llave no estará cifrada. La llave cuenta con una memoria tipo EEPROM accesible mediante distintos protocolos en serie, siendo el protocolo TWI (I2C) el que se utilizará para la autenticación. No obstante, el mismo diseño es perfectamente válido para implantar un sistema de cifrado simétrico, simplemente actualizando el programa de la cerradura y empleando una llave adecuada. Un segundo prototipo, también desarrollado en este trabajo, consistirá en la adaptación de la llave para poder usarla de manera funcional, manteniendo una comunicación sin cifrado.

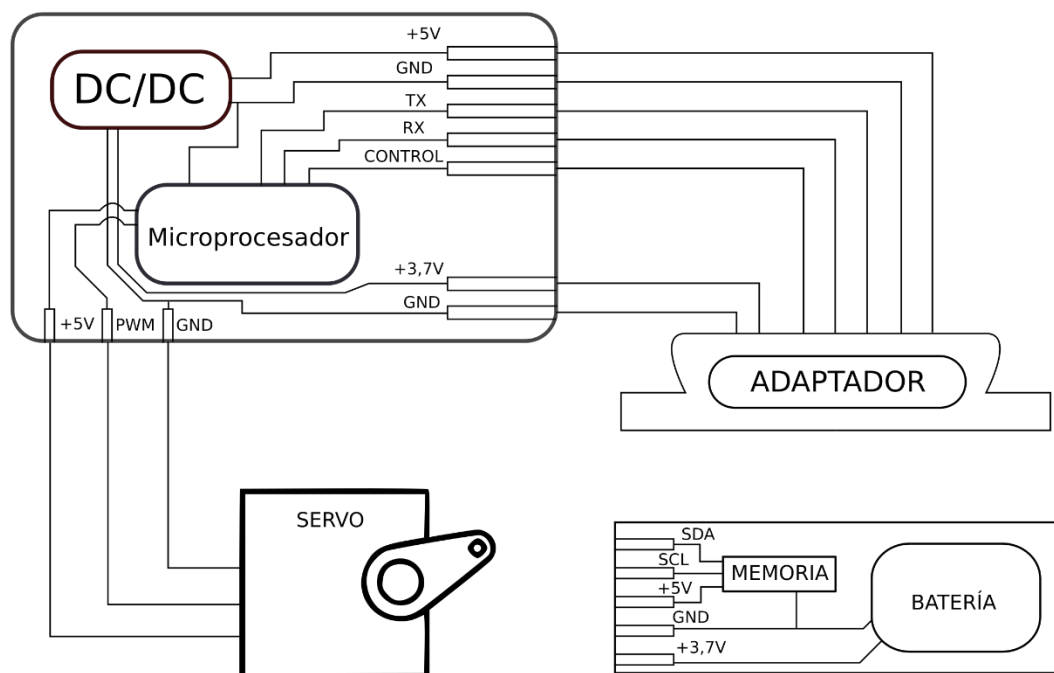
### 7.1. Diseño del prototipo

El objetivo de este prototipo es facilitar la corrección del código del programa, permitiendo probar el funcionamiento sobre la maqueta. Por ello, se ha diseñado el primer prototipo de llave empleando conectores y habilitando el acceso a todos los puertos de la memoria integrada en la llave.

En la placa se disponen dos circuitos totalmente independientes:

- Uno de ellos dispone conectores para facilitar la conexión de la batería, sin contacto alguno con la memoria integrada y facilita otro conector para suministrar la potencia a la placa principal. Este circuito es totalmente prescindible, pero se ha incluido para aproximarse a las condiciones reales de operación, dejando a la placa principal desprovista de energía hasta que se inserta la tarjeta.
- El otro circuito dispone un conector de 5 pines para la comunicación con la placa principal. En realidad, solo son necesarios 4, pero con el fin de incluir un sistema adicional de verificación para asegurar que la tarjeta está correctamente insertada, se ha incluido un pin adicional. De esta manera los pines que se pueden encontrar son: SDA, SDL, VCC, GND, GND. Además, dispone de otro puerto que permite el acceso directo a los 4 pines de la memoria que quedarían de otra manera inaccesibles.

La tensión que se suministra a la memoria son 5V, facilitados por el elevador de tensión de la placa principal. Los puertos SDA y SCL son los empleados para la comunicación serial.



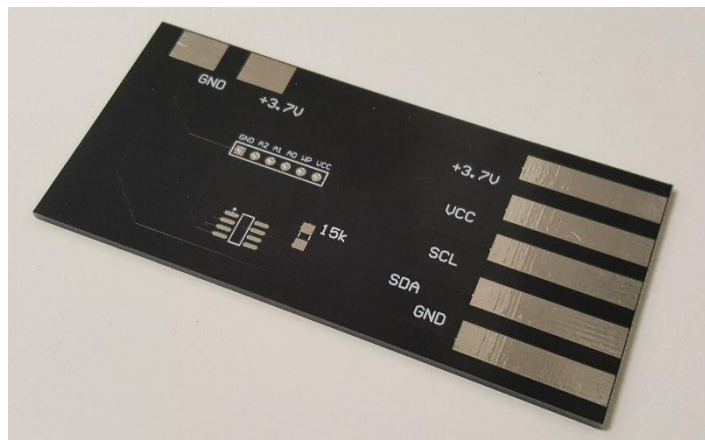
*Fig. 15: Diagrama conexiones del sistema  
(Fuente: Elaboración propia)*

La memoria dispone de un pin que permite la protección contra la escritura (WP), la cual se activará si dicho pin se encuentra a una tensión mayor de 0,5V. Resulta interesante que esta característica esté activada durante la conexión con la cerradura, no solo para evitar posibles daños a la información contenida en la llave en caso de un mal funcionamiento de la cerradura, sino de cara a una futura implantación, donde el puerto adicional que permite el acceso directo al pin WP no esté disponible. De esta manera se evita un acceso no autorizado a la llave que pueda dejarla inutilizada.

Cara a implantar dicha funcionalidad se dispone una resistencia *Pull-up* entre la pista VCC y el pin WP de la memoria, conectando directamente el pin WP, sin pasar por la resistencia, al puerto de desarrollo.

## 7.2. Comunicación TWI

Para el intercambio de información se emplea un protocolo de comunicación en serie, el cual facilita el intercambio en ambos sentidos. Para ello se ha elegido el protocolo TWI, desarrollado por Philips® con el nombre comercial I2C®. La razón de la elección de este protocolo en



*Fig. 16: Foto de la placa PCB llave definitiva  
(Fuente: Elaboración propia)*

detrimento de otros reside fundamentalmente en la necesidad de utilizar únicamente dos pines, en lugar de cuatro, tres obligatorios, del protocolo SPI. Además de TWI existen otros protocolos que emplean únicamente 2 pines, pero siendo este el más extendido y el que mayor implantación y facilidad de desarrollo tiene, se ha decidido finalmente la adopción de este sistema. Como inconveniente, cabe destacar la incapacidad del microprocesador para manejar este protocolo mediante hardware en modo anfitrión o *master*, aunque sí tiene la capacidad de hardware para manejarlo en modo esclavo. Este inconveniente no es específico del modelo elegido, sino algo generalizado en todos los microprocesadores de la gama del fabricante Atmel. A pesar de ello, existe la posibilidad de manejar dicho protocolo mediante software, procediendo de esta manera al desarrollo.

### **7.2.1. Fundamentos y operación del componente**

Como se ha indicado, el protocolo TWI hace uso de dos puertos para la comunicación, en particular son SCL y SDA, referidos al reloj y al puerto de datos respectivamente. La operación de la memoria requiere satisfacer el protocolo que estipula los tiempos y alternancia de ciclos de ambos pines.

Las transiciones de ambas líneas están definidas de manera que se asegure la validez de los datos. Dicha definición exige que el pin de datos, SDA, solo puede modificarse mientras que el reloj se encuentre en valor nulo (Tensión cero – GND).

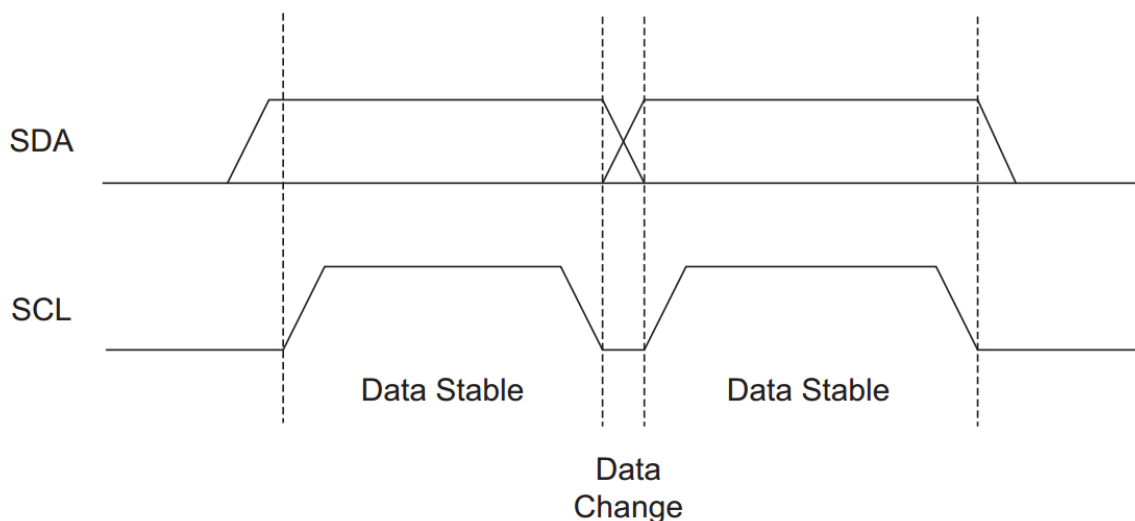


Fig. 17: Protocolo de comunicación TWI en microprocesador Atmel. Validación de datos.  
(Fuente: Atmel Corporation [10])

Además, existen otras condiciones que aseguran la validez de los datos, como son las condiciones de comienzo y final (*start & stop conditions*).

La condición de comienzo (*start*) exige que se produzca una transición de GND a VCC en la línea SDA previo a cualquier otro comando. Dicha transición se debe efectuar con la línea del reloj en posición VCC, lo cual sería una excepción a la regla de que cualquier modificación de la línea SDA requiere que el reloj se encuentre en valor nulo.

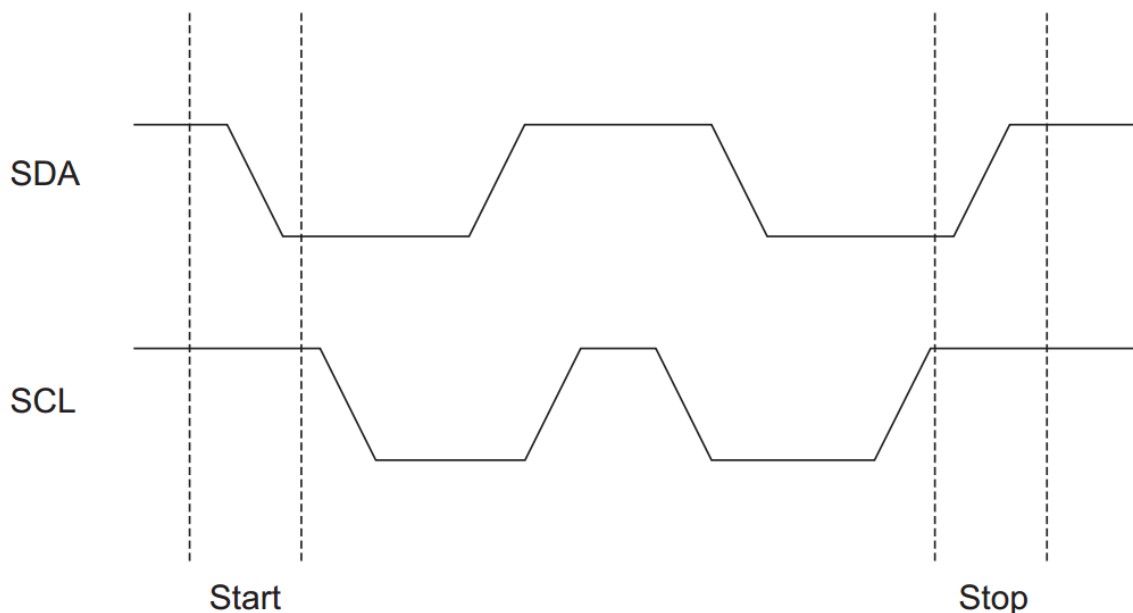


Fig. 18: Protocolo de comunicación TWI en microprocesador Atmel. Especificación de las condiciones de comienzo y fin de transmisión.  
(Fuente: Atmel Corporation [10])

La condición de final (*stop*) requiere una transición de VCC a GND de la línea SDA, con SCL en tensión (VCC), que se debe producir al final de cualquier comunicación. Dicha condición deja la memoria en estado de reposo (*stand-by mode*).

Todas las transmisiones de información, tanto direcciones como datos, se transmiten entre el maestro y el esclavo en anchos de palabra de 8 bits. Al finalizar cada transmisión se produce una pequeña comprobación que reconoce si esta se ha producido de manera adecuada. Esto ocurre durante el noveno ciclo de reloj, y se denomina *acknowledge*.

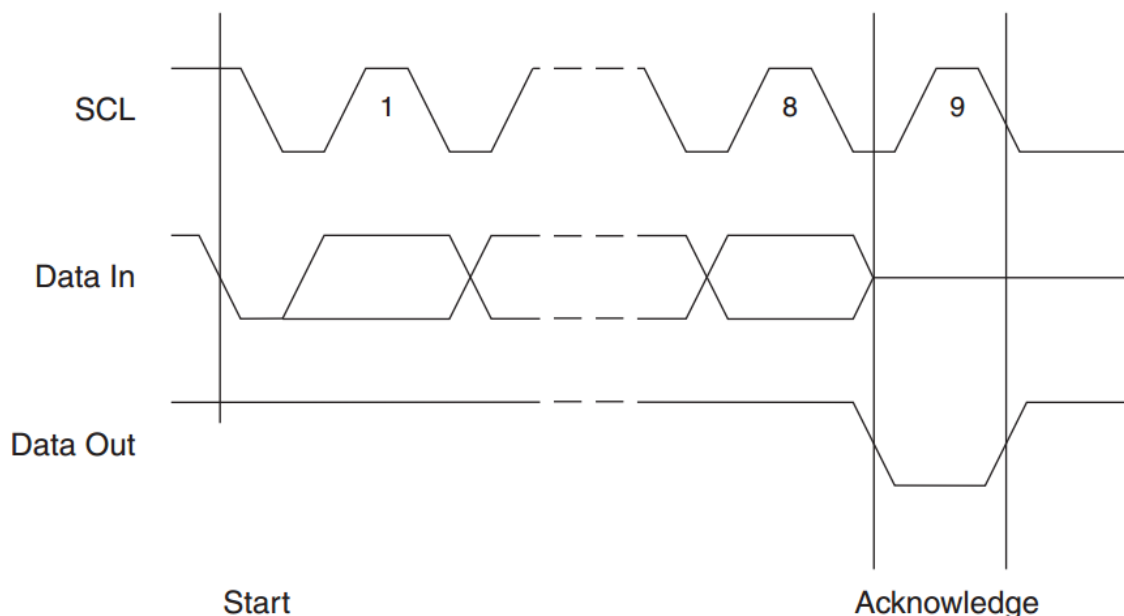


Fig. 19: Protocolo de comunicación TWI en microprocesador Atmel. Bit de comprobación.  
(Fuente: Atmel Corporation [10])

Como se ha indicado con anterioridad, existe un modo de reposo (*standby mode*), el cual se activa en la memoria al recibir la condición de “stop”, que disminuye el consumo eléctrico de la memoria. No obstante, la condición descrita no es la única que activa este estado, sino que es el estado activado por defecto al encenderse la memoria.

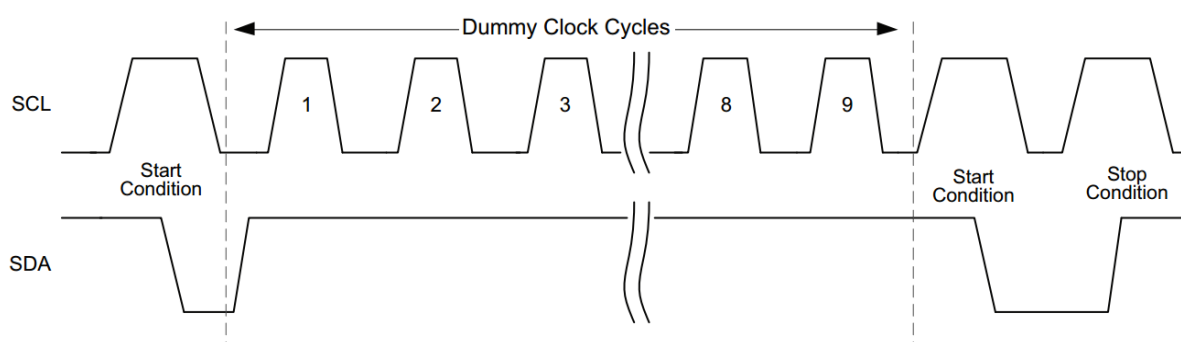


Fig. 20: Protocolo de comunicación TWI en microprocesador Atmel. Condición de reinicio.  
(Fuente: Atmel Corporation [10] [11])

Además de este modo, existen otros procesos específicos, como es el reinicio por software. Este reinicio se puede llevar a cabo tras un fallo en el protocolo, una pérdida de potencia o un reinicio inesperado del sistema, y para ello existe un protocolo serial que activa dicho reinicio. El protocolo consiste en la transmisión de una condición de comienzo (“start”), seguida de nueve

ciclos de reloj, otra condición “start” y finalmente una condición “stop”. Tras seguir estos pasos el reinicio se habrá completado y el dispositivo estará preparado para recibir un nuevo comando.

Para acceder a la memoria es necesario la transmisión de una condición de comienzo seguida de la dirección de la memoria, con un tamaño de palabra de 8 bits. Esta dirección está formada por una cadena predefinida de los 4 primeros bits '1010' (0xA), siendo los 3 bits a continuación función de los valores asignados en los pines de la memoria “A2”, “A1” y “A0”, respectivamente. El último bit corresponde al bit de selección de operación, bien sea de lectura o escritura.

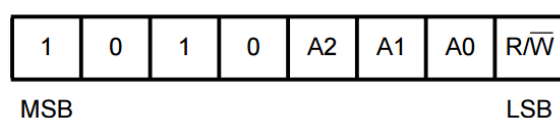


Fig. 21: Registro de acceso a la memoria  
(Fuente: Atmel Corporation [11])

Para la operación de lectura se procede incluyendo un 1 en el último bit de la cadena de direccionamiento (*addressing*). Existen tres modos de lectura, en función de la información que se desee adquirir.

De esta manera el modo principal de lectura (“*Current address read*”) se sitúa en la última posición de la memoria y devuelve el bit que se encuentra a continuación. Si se interrumpe la corriente dicha posición se reinicia.

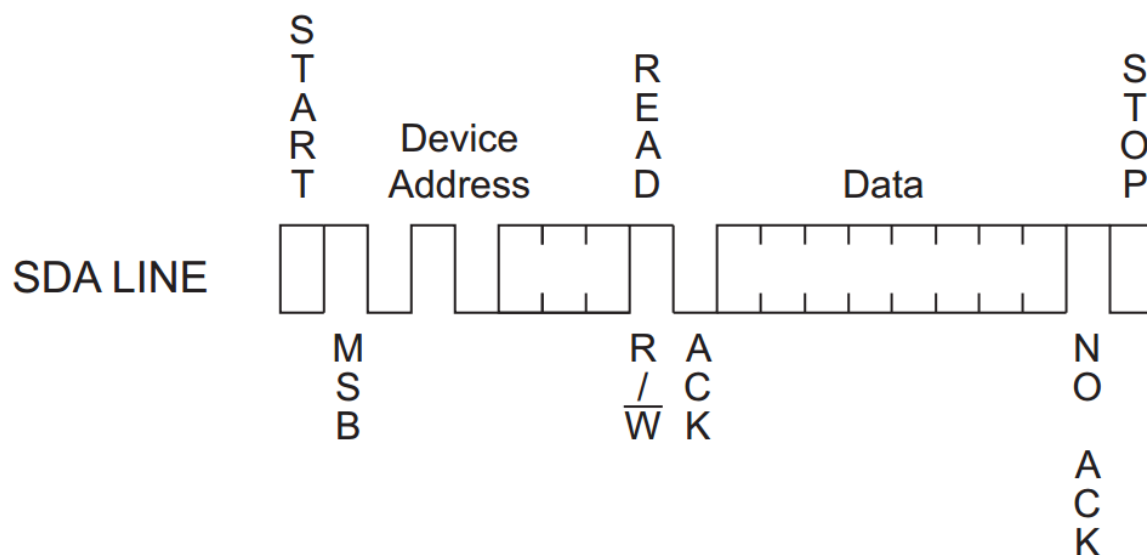


Fig. 22: Protocolo de comunicación TWI en microprocesador Atmel. Secuencia de transmisión genérica según el modo de lectura principal (“*Current address read*”)  
(Fuente: Atmel Corporation [11])



El segundo modo, “*Random read*”, accede a la posición de la memoria especificada por el dispositivo principal o maestro, y devuelve dicho valor.

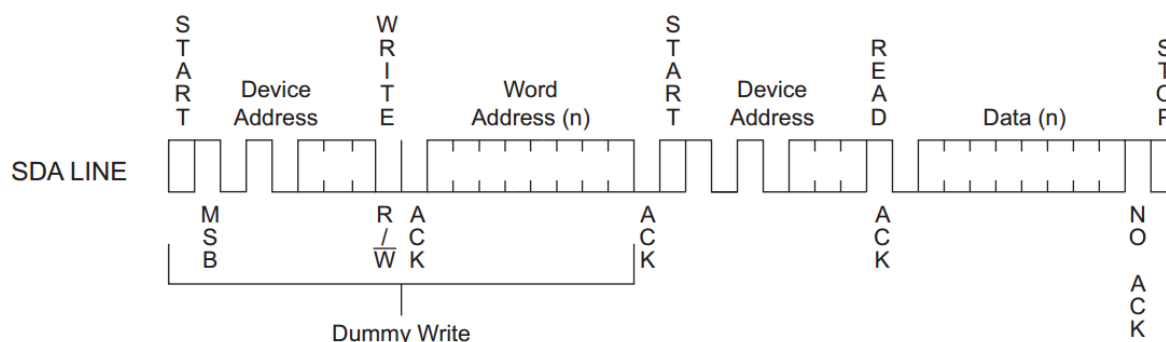


Fig. 23: Protocolo de comunicación TWI en microprocesador Atmel. Secuencia de transmisión genérica según el modo de lectura aleatorio (“*Random read*”) (Fuente: Atmel Corporation [11])

Por último, el modo secuencial, “*Sequential read*”, devuelve todo el contenido de la memoria de manera secuencial, esto es, ordenada empezando por las primeras posiciones de la memoria.

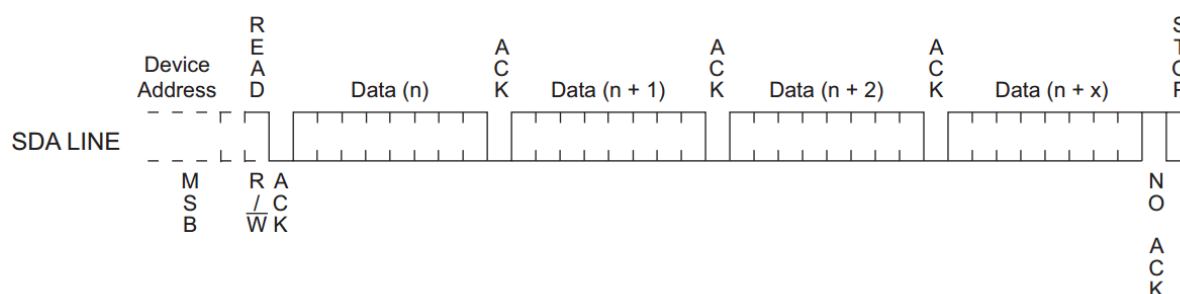


Fig. 24: Protocolo de comunicación TWI en microprocesador Atmel. Secuencia de transmisión genérica según el modo de lectura secuencial (“*Sequential read*”) (Fuente: Atmel Corporation [11])

Las operaciones de escritura no se abordarán por tratarse de un proceso de preparación previa de la llave, el cual se podría obviar en una futura producción industrial donde el propio fabricante puede incluir una clave aleatoria en la memoria. No obstante, el protocolo de escritura se detalla en la propia hoja técnica de la memoria, y resulta similar al proceso de lectura.

### 7.2.2. Programación

La programación del micro, el cual desempeñará la función de maestro en la conexión TWI, se apoya en una librería. Esto es así debido a la incapacidad del microprocesador para manejar la comunicación por hardware en modo maestro (“host”). La librería empleada esta derivada de la librería `Soft_I2C_Master` [9], la cual está escrita en C++. Debido a que la programación del microprocesador se ha realizado en C, resulta necesario la adaptación de dicha librería a este lenguaje de programación. No obstante, el fundamento y la estructura de la librería es idéntica.

Según el funcionamiento de la cerradura, únicamente será necesario acceder a la memoria en una ocasión, tras la cual se producirá la acción requerida y una vez finalizada dicha acción, el usuario retirará la llave, cortando de esta manera el suministro de corriente a la cerradura y, por tanto, también a la llave, lo que provocará el reinicio de la posición de lectura en la memoria. Este hecho condiciona la programación del microprocesador, reduciendo el tiempo de lectura y, por tanto, también el tiempo total de apertura/cierre.

En el programa principal, una vez se comprueba en qué posición se encuentra la cerradura y la puerta (abierta/cerrada), así como la correcta posición de la llave, se procede a la lectura de la memoria de la llave. Para ello se hacen tres llamadas a la librería, las cuales completan este proceso. En particular, estas tres llamadas se detallan en el Cuadro 1.

```
SoftI2cMasterInit();
key = soft_i2c_eeprom_read_byte(EEPROM_ADDR, 0);
SoftI2cMasterDeInit();
```

*Cuadro 1: Código de llamada a la librería para la comunicación TWI mediante software  
(Fuente: Elaboración propia)*

A continuación, se detalla el funcionamiento de la librería, tomando como bases los fundamentos expuestos en el apartado anterior.

En primer lugar se hace llamada a la función “*SoftI2cMasterInit()*” contenida en la librería mencionada. Esta función hace la tarea de asignar los diferentes pines necesarios para la comunicación serial y fijar valor de salida nulo (*GND*). Para la asignación se hace uso del registro “*DDRB*”, mientras que para fijar el valor se utiliza el registro “*PORTB*”.

```
void SoftI2cMasterInit(void) {
    DDRB |= (1<<TWI_SDA_PIN);
    PORTB |= (1<<TWI_SDA_PIN);
    DDRB |= (1<<TWI_SCL_PIN);
    PORTB |= (1<<TWI_SCL_PIN);
}
```

*Cuadro 2: Modificación de los registros para el acceso a la memoria  
(Fuente: Elaboración propia)*

A continuación, se llama a la función “*soft\_i2c\_eeprom\_read\_byte(A)*”, la cual requiere un parámetro, el cual consiste en la dirección de acceso a la memoria. Una vez dentro de la propia función, esta llama a su vez a distintas funciones que vienen a realizar las condiciones básicas descritas en el apartado anterior.

La primera de estas funciones es “*SoftI2cMasterStart*” que requiere de la dirección de la memoria. Esta función comienza enviando una condición de comienzo (“*start*”), definida en el apartado 5.2.1, y finaliza llamando a la función “*SoftI2cMasterWrite*” encargada de enviar los 8 bits de la dirección de la memoria, a la vez que devuelve el valor del *acknowledge* invertido, esto es, si el envío concluye de manera satisfactoria la memoria lo comunicará devolviendo un

```

uint8_t soft_i2c_eeprom_read_first_byte(uint8_t deviceAddr)
{
    uint8_t byteRead = 0;

    // Issue a start condition, send device address and
    write direction bit
    if (!SoftI2cMasterStart((deviceAddr<<1) | I2C_WRITE))
    return false;

    // Read the byte
    byteRead = SoftI2cMasterRead(1);

    // Issue a stop condition
    SoftI2cMasterStop();

    return byteRead;
}

```

*Cuadro 3: Función de la librería TWI para la lectura de un byte  
(Fuente: ---)*

valor nulo en el pin SDA, lo que debido a la programación de la función “SoftI2cMasterWrite”, esta devolverá un valor booleano *verdadero*, es decir, un 1 lógico. Este valor se devuelve a su vez al programa principal a través de la función “SoftI2cMasterStart”. De esta manera se asegura que, si el envío no concluye de manera satisfactoria, se interrumpirá el programa y devolverá un valor nulo (“false”).

```

bool SoftI2cMasterStart(uint8_t addressRW) {
    PORTB &= ~(1<<TWI_SDA_PIN);
    _delay_us(I2C_DELAY_USEC);
    PORTB &= ~(1<<TWI_SCL_PIN);
    return SoftI2cMasterWrite(addressRW);
}

```

*Cuadro 4: Función de la librería TWI encargada de iniciar el protocolo de comunicación  
(Fuente: ----)*

A continuación se llama a la función “SoftI2cMasterRead()”, la cual requiere también un parámetro y, cuyo resultado final, la lectura realizada, se almacena en la variable *byteRead*. Este procedimiento no es único, sino que depende del modo de lectura escogido. En este caso, debido a que se ha decidido proceder según el modo de lectura “*current adress read*” no es necesario enviar la posición de la memoria que se desea leer. No obstante, también se puede proceder según el modo “*random read*” que permite seleccionar la posición deseada, aun siendo esta la primera.

Dentro de la función encargada de realizar la lectura de la memoria, se comienza fijando el puerto SDA en modo entrada (*línea 3*), y activando la resistencia *Pull-Up* de dicho puerto (*línea 4*). Una vez el puerto se encuentra en modo entrada (*INPUT*), se procede a la lectura de los 8 bits mediante un bucle *for*, el cual procede a guardar el valor leído bit a bit, identificando cada

nuevo bit por el ciclo de reloj controlado por el microprocesador. Por último, en función del parámetro proporcionado a esta función se modifica el modo del pin SDA (entrada/salida),

```
uint8_t SoftI2cMasterRead(uint8_t last) {
    uint8_t b = 0;
    PORTB |= (1<<TWI_SDA_PIN);
    DDRB &= ~(1<<TWI_SDA_PIN);
    for (uint8_t i = 0; i < 8; i++) {
        b <=< 1;
        _delay_us(I2C_DELAY_USEC);
        PORTB |= (1<<TWI_SCL_PIN);
        if (bit_is_set(PINB, TWI_SDA_PIN)) b |= 1;
        PORTB &= ~(1<<TWI_SCL_PIN);
    }
    DDRB |= (1<<TWI_SDA_PIN);
    if (last) {
        PORTB |= (1<<TWI_SDA_PIN);
    }
    else {
        PORTB &= ~(1<<TWI_SDA_PIN);
    }
    PORTB |= (1<<TWI_SCL_PIN);
    _delay_us(I2C_DELAY_USEC);
    PORTB &= ~(1<<TWI_SCL_PIN);
    PORTB &= ~(1<<TWI_SDA_PIN);
    return b;
}
```

*Cuadro 5: Función de la librería TWI encargada de leer el dato recibido de la memoria.  
(Fuente: ----)*

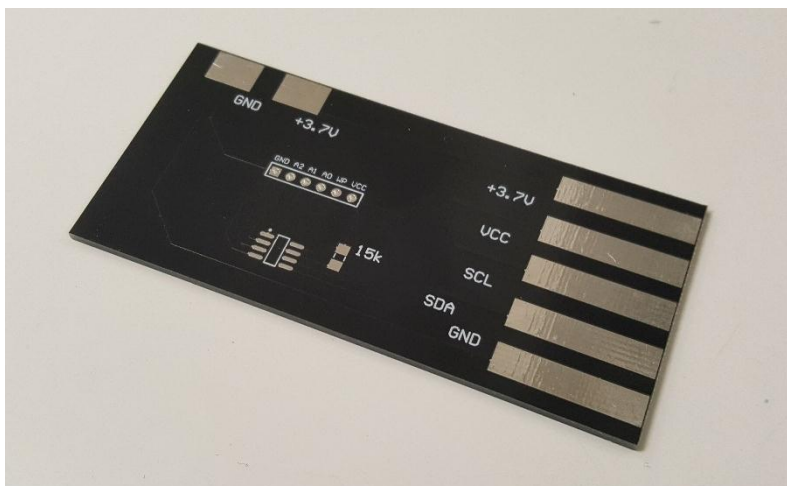
dependiendo de si el byte leído es el último o no, y se devuelve el valor leído.

Para finalizar se llama a la función “*SoftI2cMasterStop()*” la cual produce una condición “*stop*”, provocando que la memoria entre en el modo de reposo (*standby*). Para ello se procede según el protocolo descrito en el apartado 5.2.1. Una vez enviada la condición de “*stop*” solo queda liberar los pines utilizados para la comunicación, aunque este es un paso totalmente opcional. Para ello se puede llamar a la función “*SoftI2cMasterDeInit()*”.

### 7.2.3. Diseño prototipo funcional

```
void SoftI2cMasterStop(void) {
    PORTB &= ~(1<<TWI_SDA_PIN);
    _delay_us(I2C_DELAY_USEC);
    PORTB |= (1<<TWI_SCL_PIN);
    _delay_us(I2C_DELAY_USEC);
    PORTB |= (1<<TWI_SDA_PIN);
    _delay_us(I2C_DELAY_USEC);
}
```

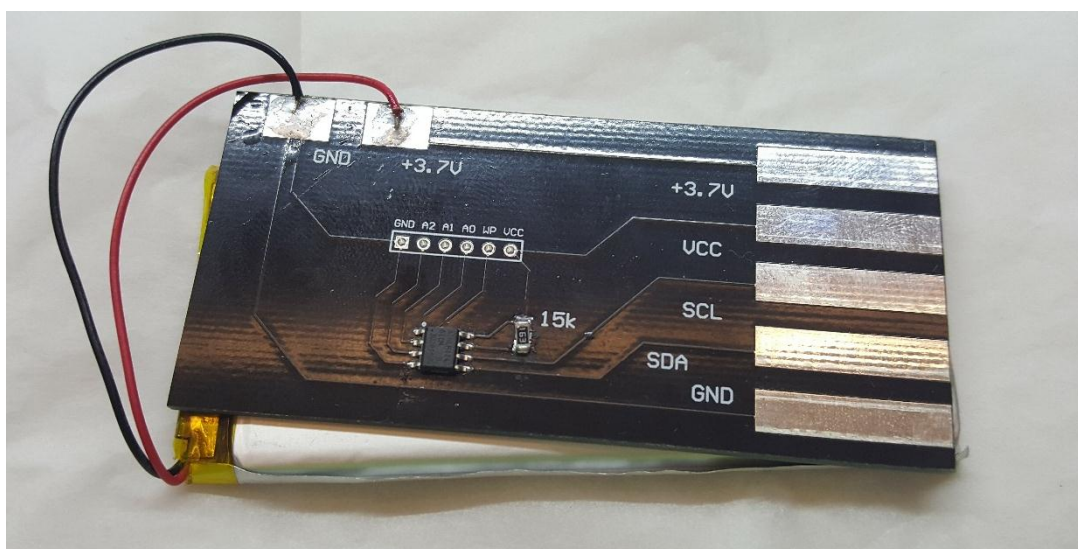
*Cuadro 6: Función de la librería TWI encargada de detener la comunicación.  
(Fuente: Librería SoftI2cMaster [9])*



*Fig. 25: Fotografía de la placa PCB prototipo. Se pueden distinguir las huellas para soldar la memoria y la resistencia pull-up  
(Fuente: Elaboración propia)*

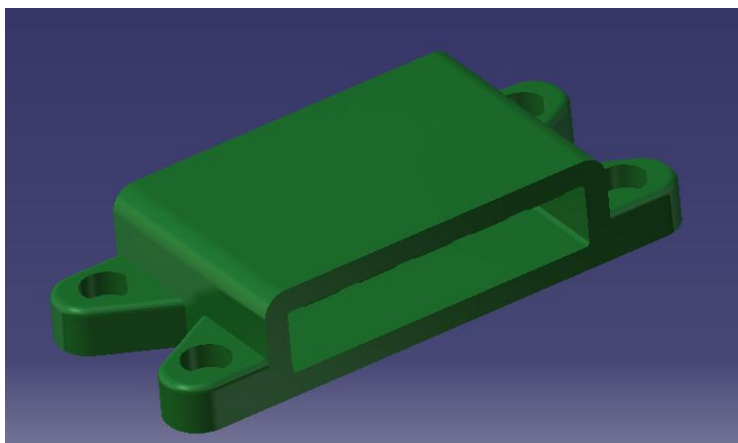
Para el diseño de la llave es fundamental tener en cuenta las exigencias debidas al protocolo de comunicación empleado, así como a las características intrínsecas del sistema. En este apartado no se va incidir sobre el dimensionamiento mecánico, el cual ya se ha abordado en el capítulo correspondiente, pero si se van a asumir los resultados para fundamentar las decisiones adoptadas.

Como ya se ha detallado, el protocolo TWI requiere 2 líneas para la transmisión de datos, a las cuales se deben añadir irremediabilmente las líneas de alimentación. De esta manera, se deben disponer al menos 4 líneas para la comunicación con la memoria, teniendo en cuenta que se quisiera conectar de una manera habitual. No obstante, el caso que aquí se trata es diferente, pues además de almacenar la clave de apertura, la llave tiene otra función de gran relevancia, como es la provisión de energía a todo el sistema.



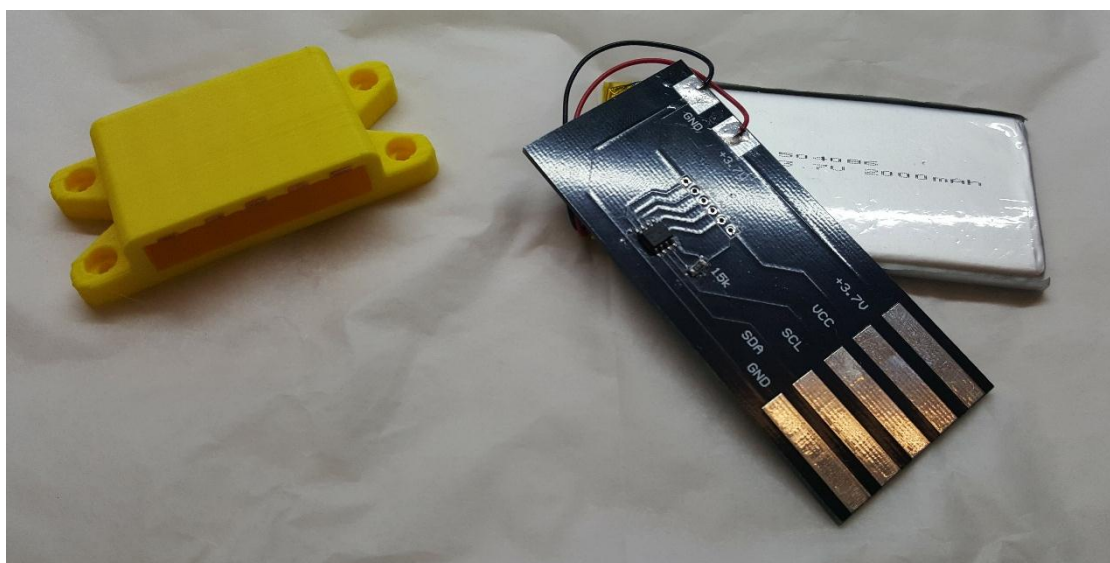
*Fig. 26: Fotografía de la tarjeta llave, compuesta por la placa PCB y la batería. Se pueden apreciar los componentes soldados a la placa  
(Fuente: Elaboración propia)*

Dada esta situación, es necesario disponer un canal adicional que permita alimentar al sistema desde la llave, para lo cual suelen ser necesarias 2 líneas. En este caso, para reducir el sistema y, dado que el elevador de tensión comparte la misma línea de tierra para la entrada y la salida, se ha optado por emplear una única conexión de tierra, reduciendo el número final de líneas a 5. Este montaje difiere del primer prototipo en que se ignora la línea de comprobación, la cual se puede añadir sobre el propio soporte con posterioridad y permite mejorar el contacto de las líneas al aumentar el ancho y la distancia entre ellas.



*Fig. 27: Imagen renderizada del soporte diseñado en CATIA  
(Fuente: Elaboración propia)*

Para la lectura de la tarjeta se ha diseñado un soporte con un software CAD (CATIA V5), de manera que permita un contacto preciso entre soporte y tarjeta. Este montaje conlleva cierta dificultad, ya que una pequeña holgura entre ambas partes puede ocasionar un mal contacto de alguna de las líneas, provocando, por tanto, un mal funcionamiento del sistema. Por esta razón, adquiere mayor relevancia el proceso de fabricación del soporte, dado que determinará el ajuste que se puede conseguir.



*Fig. 28: Fotografía del soporte fabricado mediante impresión 3D y la tarjeta llave.  
(Fuente: Elaboración propia)*



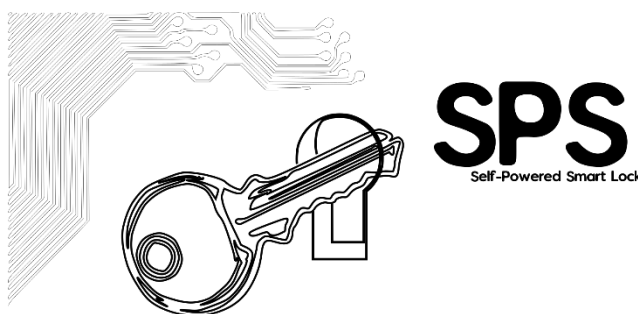
Para fabricar el soporte se ha empleado una impresora 3D de fabricación casera (DIY), la cual dispone de una precisión de 100 micras. Se ha tenido en cuenta el espesor conjunto de batería y tarjeta, el cual conformará la llave y en función de éste y el resto de dimensiones de la batería, se han diseñado tanto el soporte como la tarjeta. Para asegurar el ajuste, se ha realizado una leve inclinación de los contactos del soporte, de tal manera que, con la llave introducida en el soporte, la presión sobre los contactos sea máxima en la punta. Esto se consigue determinando una abertura en el fondo del soporte levemente menor que el espesor de la tarjeta.



*Fig. 29: Fotografía del soporte fabricado mediante impresión 3D. Se pueden apreciar las tiras de cobre para el contacto con la placa  
(Fuente: Elaboración propia)*

Una vez impreso el soporte, se procede a la colocación de tiras de cobre a modo de contactos sobre el soporte. Estas tiras disponen de adhesivo en una cara, de tal manera que facilita su colocación y uso ya que su posición quedará fijada, sin correr el riesgo de que se produzca un arrastre de la tira al introducir la llave. Puede resultar interesante destacar la mayor eficiencia de los adhesivos en este tipo de situaciones, cuando la dirección de la fuerza aplicada está contenida en la superficie adhesiva.

Para la conexión del soporte a la placa de procesamiento, se dispone de ciertos agujeros en el fondo del soporte, los cuales permiten la continuidad de las tiras de cobre por el exterior, facilitando la soldadura posterior de los cables que lo conectarán con dicha placa.



*Fig. 30: Imagen vectorial del logotipo. Diseñada con Inkscape  
(Fuente: Elaboración propia)*

El diseño de la tarjeta definitiva se ha realizado empleando ALTIUM, un software específico para el diseño de PCBs. También se ha realizado un logotipo grabado sobre el reverso de las tarjetas, con la finalidad de crear una imagen identificativa del proyecto. Para su realización se ha utilizado un software de diseño vectorial de código libre (Inkscape) y se han elegido, así mismo, las siglas “SPS”, tomando las iniciales de “Self-Powered Smart Lock”, lo que en español se puede traducir como “*Cerradura Inteligente auto-alimentada*”, pretendiendo de esta manera resaltar sus características más distinguidas, como son, la capacidad de automatización y control y el sistema de alimentación a través de la propia tarjeta.



*Fig. 31: Fotografía de la placa PCB con la imagen del proyecto. Se puede leer “SPS – Self-Powered Smart Lock”  
(Fuente: Elaboración propia)*



## **8. CONCLUSIONES**



## 8 CONCLUSIONES Y VALORACIÓN

### 8.1. Conclusiones

En este apartado se pretende hacer una recopilación de los objetivos propuestos y del grado de efectividad logrado en su consecución. Para ello, se enumeran de nuevo dichos objetivos con el fin de poder realizar dicha valoración:

- Diseño y fabricación de un sistema de cierre electrónico con las siguientes características:
  - Accionamiento electromecánico
  - Posibilidad de instalación sobre plataformas existentes
  - Diseño orientado a futuras mejoras y modularidad
  - Bajo coste

El prototipo desarrollado, como se ha podido comprobar a lo largo de la presente memoria, cumple estos objetivos de manera absoluta. El accionamiento elegido es capaz de adaptarse a cualquier plataforma existente mediante el aplique adecuado, sin requerir ninguna modificación de la puerta y todo ello por un precio muy reducido, inferior incluso al de una cerradura convencional. Además, gracias al enfoque que se ha establecido desde el principio orientado a la modularidad y a la posterior mejora del sistema, se abre la posibilidad de incorporación de múltiples funcionalidades adicionales.

- Fabricación de un prototipo funcional que permita la operación de una cerradura en condiciones de operación real.

Este objetivo se ha conseguido de manera completa, ya que el prototipo diseñado es capaz de accionar la cerradura de manera completa, ejecutando ciclos de apertura y cierre según lo esperado. El soporte fabricado permite, a su vez, un uso sencillo de la cerradura que perfectamente se podría emplear en un entorno real, siempre y cuando se mejorara el diseño para evitar un desgaste excesivo u otros problemas debidos al uso continuado.

- Programar el sistema para permitir la operación en condiciones reales, estableciendo la comunicación entre cerradura y llave, sentando la base para desarrollos futuros.

El prototipo fabricado es capaz de funcionar con total operatividad y, gracias a la programación implementada, sería posible su instalación en cualquier puerta asegurando un funcionamiento fiable. No obstante, este objetivo no se puede considerar como absolutamente conseguido, pues unas condiciones de operación reales requerirían unos niveles de seguridad muy elevados, lo

que hace indispensable la incorporación de un sistema de cifrado que asegure el proceso de autenticación. Aunque esto se pueda considerar como una limitación, realmente no lo es, pues la no incorporación de un sistema de cifrado ha sido una decisión deliberada con el fin de facilitar la incorporación posterior de cualquier tipo de cifrado, no limitando la adopción de una tecnología en detrimento de otra.

- Dimensionar el par necesario para la operación de una puerta de seguridad mediante accionamientos electromecánicos, ofreciendo datos fiables para futuras consultas.

El método empleado para el dimensionamiento se puede mejorar utilizando otro tipo de herramientas que permitan, no solo una mayor precisión de medida, sino una medición del par resistivo instantáneo en todo momento, a diferencia del método empleado que solo permite obtener el valor del par máximo. A pesar de esta limitación, y como ya se ha detallado en el apartado **¡Error! No se encuentra el origen de la referencia.**, los datos obtenidos son suficientemente fiables ya que ofrecen una cota superior y, por tanto, un margen de seguridad que siempre es importante, pero más aún en aquellos sistemas que van a estar sometidos a condiciones de operación de muy diversos tipos.

### 8.2. Valoración de impactos

Como se ha explicado a lo largo del presente trabajo, la seguridad de los sistemas empleados tanto en domicilios como en pequeñas y medianas empresas se considera, en la actualidad, muy vulnerable. Ciertos estudios llegan a situar el número de cerraduras domésticas vulnerables al *bumping* en un 90% [2]. Ante esta situación se hace obvia la gran influencia social, económico e incluso, cultural, que puede llegar a suponer este trabajo, ya que la innovación en el campo de la seguridad es fundamental para garantizar el desarrollo de la sociedad.

Este trabajo presenta una idea innovadora que pretende facilitar la transición a los sistemas de cierre basados en autenticación electrónica, aumentando de esta manera la seguridad a la vez que se reducen los costes de las cerraduras, facilitando su adquisición por parte de todos los estratos sociales.

Por otro lado, todo el trabajo desarrollado ha servido para generar una documentación que, con seguridad, servirá para futuros desarrollos en este campo, a la vez que facilitará la mejora del presente sistema. La necesidad de fabricar un sistema de medición del par para poder medir aquellos valores necesarios para parametrizar la cerradura y poder dimensionar su accionamiento, disminuye el alcance de cualquier proyecto, debido a los elevados recursos que consume. Por esta misma razón, el presente trabajo se convierte en una valiosa documentación de referencia para futuros proyectos de cerraduras electrónicas motorizadas.

Por último, indicar que todo el desarrollo del proyecto ha transcurrido con el máximo respeto ambiental, garantizando el mínimo desperdicio de recursos, así como asegurando el correcto reciclaje de aquellos recursos que habiendo sido utilizados, ya no eran necesarios.

## **9. LÍNEAS FUTURAS**



## 9 LÍNEAS FUTURAS

Como se ha indicado en la introducción, el presente proyecto se ha desarrollado con la idea de servir de base sobre la cual poder implementar otros sistemas que aumenten las funcionalidades. De esta manera, el proyecto se convierte en los cimientos de una torre, gracias a los cuales se asegura que esta podrá ser tan alta como sea necesario.

La adopción de este planteamiento desde un principio no significa que el autor obvie las diferentes implantaciones de cerraduras electrónicas existentes en la actualidad, sino que se refuerza la importancia de disponer de una base sólida sobre la que implantar aquellas.

En este apartado se abordarán aquellas líneas futuras que se consideran más en orden con las tendencias actuales, aportando las más demandadas características por parte del usuario, como pueden ser automatización, identificación sin contacto, gestión remota, etc.

### 9.1. Innovaciones en la autenticación

Una de las características más en auge actualmente consiste en el empleo de sistemas de radiofrecuencia para el intercambio de información entre dispositivos. Estos sistemas consiguen realizar la comunicación sin necesidad de contacto físico, aunque este a veces se mantiene por razones de diseño.

De esta manera, existen soluciones pensadas para permitir la comunicación cuando los dispositivos están a pocos centímetros de distancia entre sí, idóneos para tareas de identificación personal como es el del dispositivo aquí desarrollado. A pesar de no ser necesario el contacto, existen soluciones donde se sigue requiriendo debido al propio diseño o a características particulares. Un ejemplo de esta solución pueden ser las cerraduras de los automóviles modernos, que presentan una doble autenticación mecánica y electrónica, aunque la comprobación electrónica solo se realiza una vez validada la primera.

Por otro lado, existen otras soluciones ideadas para otros rangos de longitud, consiguiendo así adaptarse a diferentes aplicaciones y requerimientos.

Además de la particular comodidad que aportan dichos sistemas, presentan otras muchas ventajas, las cuales justifican la amplia aceptación que reciben en la actualidad por parte de todos los sectores. Algunas de estas ventajas son: ausencia de desgaste al no requerir contacto, alimentación pasiva, donde el emisor proporciona la energía suficiente como para que el receptor no requiera otra fuente de alimentación, delimitación del rango de acción mediante un diseño adecuado, lo que protege del robo de información, así como aumenta las posibilidades del sistema.

Además de los sistemas de comunicación inalámbricos por radiofrecuencia o acoplamiento magnético, existen otros métodos con un creciente desarrollo, como son aquellos que funcionan

mediante imagen, con códigos QR, o sonido, mediante emisión acústica en frecuencias no audibles. Estos sistemas, pese a proporcionar unos niveles de seguridad y efectividad muy elevados, muchas veces incluso superiores a los sistemas por radiofrecuencia, tienen la limitación de no poder transmitir energía, lo que obliga a la incorporación de una fuente de alimentación específica para el receptor.

Otros mecanismos de autenticación que están cobrando especial importancia en la actualidad son aquellos que emplean parámetros biométricos como elementos de validación. Un ejemplo serían los escáneres dactilares presentes en la mayoría de los teléfonos móviles que se pueden encontrar en estos días en el mercado. Pero no solo se pueden utilizar las huellas de las manos para la identificación, sino que existen numerosos rasgos en cada persona que resultan únicos y, por tanto, su correcta medición permite la identificación unívoca de los individuos.

De esta manera, se han desarrollado en la actualidad todo tipo de sensores que permiten el análisis de parámetros biométricos complejos como pueden ser los rasgos de la cara, la forma del iris, el ADN o, incluso, el ritmo cardíaco. Además del rango de funcionamiento del sensor, cobra especial importancia su funcionamiento interno ya que es el que acaba delimitando en gran medida su eficacia. Así se pueden encontrar varios sensores para la misma aplicación, pero con un funcionamiento radicalmente distinto. Un ejemplo representativo de esta circunstancia se puede encontrar en los mismos sensores dactilares, donde existen dos tecnologías principales, una óptica y otra acústica.

Esta circunstancia se produce en todo tipo de ámbitos, no solo en los sensores biométricos, aunque resulta evidente que es mayor en aquellos sectores que gozan de gran inversión e interés comercial. Esta amplitud de soluciones proporciona una seguridad muy elevada en la autenticación, al implementar diferentes validaciones de manera simultánea. No obstante, adolecen de una carencia importante, ya que están enfocados a la medición de datos y no disponen un mecanismo de intercambio de energía. Además de no disponerlo, tampoco se concibe, ya que están diseñados de una forma general para abarcar múltiples escenarios.

De esta manera, resulta evidente la mejora de seguridad que supone añadir más sistemas de validación, como pueden ser los ya mencionados, pero siempre de manera adicional, ya que resulta imprescindible, debido a como se ha diseñado el sistema, el uso de una tarjeta de autenticación que disponga de energía suficiente como para alimentarlo.

En definitiva, la implementación de sistemas de autenticación adicionales, no solo es una posibilidad, sino que debería convertirse en uno de los atractivos principales de este sistema. La manera óptima de enfocar este desarrollo, según la visión del autor del presente proyecto, consistirá en módulos adicionales que se podrán acoplar al sistema principal para añadir funcionalidades específicas, pero manteniendo las ventajas del sistema original. Un ejemplo podría ser la implementación de una cámara con procesamiento de imágenes para el reconocimiento facial. Así, al autenticarse con la tarjeta de acceso, la propia energía acumulada en ella sea suficiente como para alimentar este sistema auxiliar de reconocimiento facial, incluyendo así mismo todos los subsistemas.



Con esta idea, resulta evidente la dirección que deben tomar los desarrollos futuros, centrando la atención de manera especial sobre el sistema de almacenamiento de carga, que debe dar soporte a todo el sistema, la eficiencia del mecanismo y de los subsistemas de validación alternativos que influirá de manera decisiva sobre el consumo de potencia y, por tanto, sobre la energía que debe almacenar la tarjeta y, por último y no por ello menos importante, sobre el cifrado de las conexiones y la seguridad de los sistemas de autenticación alternativos.

## 9.2. Automatización y gestión remota

Gracias al enorme desarrollo de la electrónica y la consiguiente reducción de tamaño y coste de los equipos, se ha llegado a una situación donde resulta rentable la automatización de prácticamente cualquier sistema. Llegado a este punto, el desarrollo no depende tanto de los sistemas físicos, sino de la programación de estos. De esta manera, disponer un hardware mínimo es base suficiente para desarrollar un sinnúmero de aplicaciones sobre este.

En este proyecto se pretende asentar una base mínima sobre la cual se puedan implementar diferentes soluciones de software en capas superiores, ampliando las posibilidades del sistema hasta el límite que sea necesario para satisfacer las necesidades del usuario. Por ello, resulta de gran interés el continuo desarrollo de la presente propuesta con el fin de añadir las capacidades de hardware, permitiendo una mayor amplitud de aplicaciones.

La instalación de un sistema de comunicación que permita el acceso a Internet, bien sea de manera alámbrica o inalámbrica, permitirá el desarrollo de aplicaciones de control remoto, o incluso la inclusión de estos sistemas en redes para permitir el control a gran escala. Además de estos sistemas de comunicación, también tendrían sentido aquellos de corto alcance, bien mediante una conexión “*ad-hoc*” con dispositivos móviles, o bien mediante la conexión a redes locales, con el fin de permitir un control avanzado de funciones, así como la programación del sistema.

Las aplicaciones de control remoto son una realidad en muchas cerraduras electrónicas del mercado, por lo que la inclusión de estas aplicaciones en el presente sistema sería una tarea lógica y sencilla, pero que añadiría gran valor.

En cuanto al acceso a redes, es interesante destacar las enormes posibilidades que una conexión de este tipo conllevaría. Por un lado, el control de grandes instalaciones se vería simplificado en gran medida al incluir todos los sistemas de cierre en una misma red centralizada, cuyo nodo central fuera capaz de gestionar los diferentes accesos de manera inteligente, pero a la vez, operando cada cerradura de manera autónoma, consiguiendo de esta manera reducir las consecuencias de un fallo de red.

Por otro lado, el gran desarrollo de las redes distribuidas, muy representativas en entornos de alta fiabilidad y/o disponibilidad, añade aún más posibilidades a estos sistemas. La inclusión de

sistemas de cierre inteligentes en una red de este tipo conferiría unas capacidades de gestión y automatización muy avanzadas con una inversión mínima, al no requerir potentes servidores centrales, a la vez que se amplía la disponibilidad y se reduce la posibilidad de fallo del sistema y, por tanto, inoperatividad.

Este último punto invita a pensar en la tecnología Blockchain como una implementación lógica para estos sistemas, que acabaría otorgando unas capacidades sin precedentes a lo que desde siempre han sido sistemas caracterizados por la sencillez, pero cuya optimización puede conllevar grandes beneficios. La posibilidad de gestión de las cerraduras inteligentes de manera descentralizada o distribuida, pero segura, de tal manera que cada operación sobre el sistema quede completamente validada, es la traducción de lo que podría ser un perfecto sistema basado en Blockchain, donde la operación quede firmada por la persona con derechos sobre la cerradura, y sea esta la que se encargue de validar dicha firma mediante la clave pública de dicha persona.

De igual manera, resultan evidentes las posibilidades que dichos sistemas conllevarían de cara a la optimización de todas las tareas, abriendo la posibilidad de que sea la propia cerradura la que se auto-gestione, generando operaciones, peticiones y publicaciones utilizando su propia clave única identificativa. Un ejemplo de esta implementación puede ser la emisión por parte de la cerradura de un aviso de intento de robo a las autoridades pertinentes, al detectarlo mediante los sensores instalados en la misma. En esa situación la cerradura procedería a emitir una publicación firmada, la cual puede ser fácilmente verificada por cualquier entidad y, por tanto, se hace posible la validación de la información de una manera unívoca.

## **10. PLANIFICACIÓN TEMPORAL Y PRESUPUESTO**



## 10 PLANIFICACIÓN TEMPORAL Y PRESUPUESTO

En este apartado se detalla la planificación seguida desde el comienzo, la cual ha permitido optimizar las tareas y seguir un desarrollo lógico durante toda la duración del proyecto. Para ello se ha descompuesto el proyecto siguiendo un organigrama EDP (Fig. 32: EDP del proyecto) que permite la visualización de las principales tareas organizadas por fases.

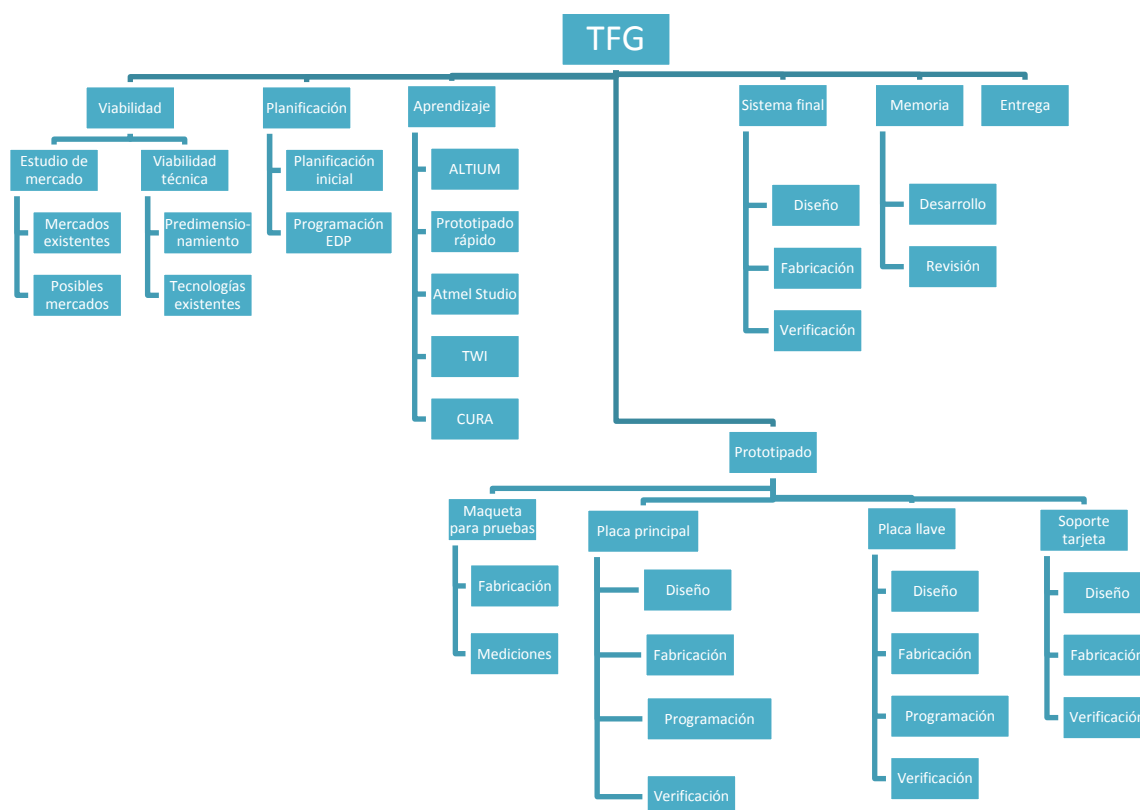


Fig. 32: EDP del proyecto  
(Fuente: Elaboración propia)

El diagrama EDP, si bien permite la visualización de las principales fases del proyecto desglosadas en tareas básicas, no muestra la evolución en el tiempo de cada fase, lo cual impide realizar una planificación adecuada en función del tiempo. Por ello, se ha desarrollado un diagrama de Gantt cuyas etapas se corresponden con el anterior.

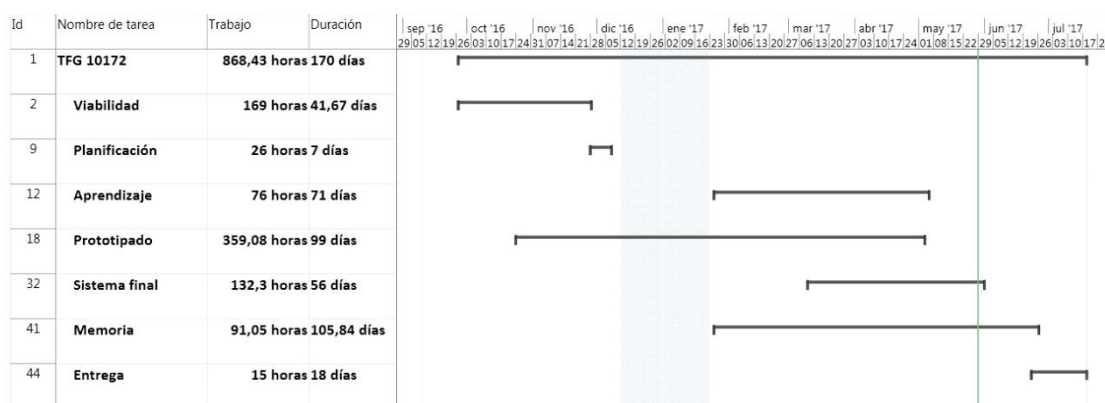
En primer lugar, se ha procedido a realizar un estudio de viabilidad con el fin de entender el mercado y las soluciones existentes, pero, también, de obtener ciertas medidas que han permitido pincelar lo que sería el diseño a desarrollar. Una vez sentada esta base, ya es posible establecer las distintas fases del proyecto, así como las tareas principales y prever una duración estimada de estas. Este trabajo es el que ha permitido elaborar el diagrama EDP y, de manera consecutiva, la planificación del proyecto.

Estas fases se especifican en la Tabla 9, donde además se puede consultar la fecha de inicio y fin, la duración y el coste estimado de cada fase, y también del proyecto en su totalidad. Estos costes se deben, de manera mayoritaria, a los recursos humanos que han participado en el desarrollo del proyecto. No obstante, no son estos los únicos recursos, ya que además se han

Nombre	Comienzo	Fin	Duración	Costo
TFG 10172	mar 27/09/16	mar 18/07/17	170 días	13.846,57 €
Viabilidad	mar 27/09/16	lun 28/11/16	41,67 días	2.755,00 €
Planificación	lun 28/11/16	mié 07/12/16	7 días	390,00 €
Aprendizaje	mié 25/01/17	vie 05/05/17	71 días	1.140,00 €
Prototipado	lun 24/10/16	mié 03/05/17	99 días	5.396,37 €
Sistema final	vie 10/03/17	mié 31/05/17	56 días	2.374,41 €
Memoria	mié 25/01/17	lun 26/06/17	105,84 días	1.565,79 €
Entrega	vie 23/06/17	mar 18/07/17	18 días	225,00 €

*Tabla 9: Fases del proyecto y coste real desglosado para cada fase.  
(Fuente: Elaboración propia)*

empleado equipos con una disponibilidad limitada cuyo uso tiene un elevado coste asociado. Para realizar el cálculo de costes de la manera más precisa posible, se ha utilizado la tasa estándar media que empresas especializadas cobran por el uso de estos servicios, y se ha representado en la Tabla 10.



*Fig. 33: Diagrama de Gantt resumen  
(Fuente: Elaboración propia)*

De manera adicional, en la Tabla 10 se puede consultar el trabajo real empleado por cada recurso en horas, así como el coste total de cada uno de ellos. Cabe mencionar el excesivo tiempo de trabajo empleado por el alumno, en comparación con lo que se estima debe ser la duración del presente trabajo. La razón fundamental de este exceso de tiempo es la fabricación del sistema en miniatura sobre el cual realizar las pruebas de funcionamiento. Esta tarea queda totalmente

fuera del objetivo del trabajo y no pretende desarrollar ni asentar ninguna competencia obtenida, por lo que se desarrolla de manera totalmente adicional con el fin de facilitar las pruebas y verificar el correcto funcionamiento de una manera intuitiva.

Nombre	Costo	Trabajo	Tasa estándar
Alumno	10.206,57 €	680,43 horas	15,00 €/hora
Fresadora de PCBs	600,00 €	60 horas	10,00 €/hora
Impresora 3D	40,00 €	8 horas	5,00 €/hora
Tutor	3.000,00 €	120 horas	25,00 €/hora

*Tabla 10: Recursos del proyecto y coste de los mismos  
(Fuente: Elaboración propia)*

Por último, en la Fig. 33 se puede consultar el resumen del diagrama de Gantt del proyecto, el cual muestra las fases principales, el trabajo y duración. Para consultar el diagrama de Gantt completo se puede acudir al Diagrama de Gantt.





## **11. REFERENCIAS**



## 11 REFERENCIAS

- [1] Ministerio de Defensa, Octubre 2009. [En línea]. Available: [http://www.tecnologiaeinnovacion.defensa.gob.es/Lists/Publicaciones/Attachments/13/monografia\\_sopt\\_2.pdf](http://www.tecnologiaeinnovacion.defensa.gob.es/Lists/Publicaciones/Attachments/13/monografia_sopt_2.pdf). [Último acceso: 4 Junio 2017].
- [2] KABA, «KABA,» [En línea]. Available: <http://www.kaba.es/22562-23972/el-metodo-bumping-un-arma-de-doble-filo.html>. [Último acceso: Junio 2017].
- [3] «SUCARMO,» [En línea]. Available: <http://www.ganzuas-picks.es/extractor-cilindros-p-48.html?osCsid=70ec0743aa7e3465952645403b8299e6>.
- [4] E. C. M. BSc. [En línea]. Available: <http://www.learnabout-electronics.org/PSU/psu32.php>.
- [5] ATMEL, «tinyAVR,» [En línea]. Available: <http://www.atmel.com/products/microcontrollers/avr/tinyavr.aspx>.
- [6] ATMEL, «AVR Dragon,» [En línea]. Available: <http://www.atmel.com/webdoc/avrdragon/index.html>.
- [7] ATMEL, «picoPower,» [En línea]. Available: <http://www.atmel.com/technologies/lowpower/picopower.aspx>.
- [8] LINEAR TECHNOLOGY, [En línea]. Available: <http://cds.linear.com/docs/en/datasheet/3529fb.pdf>.
- [9] T. E. Kurt, *Libreria SoftI2C Master*, 2010-2012.
- [10] appusajeev. [En línea]. Available: <https://appusajeev.wordpress.com/2010/09/30/pwm-in-avr/>.
- [11] ATMEL, «ATtiny 441 Datasheet,» [En línea]. Available: [https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiM3uGIh6XUAhUEJVAKHQmaBooQFggqMAA&url=http%3A%2F%2Fwww.atmel.com%2FImages%2FAtmel-8495-8-bit-AVR-Microcontrollers-ATtiny441-ATtiny841\\_Datasheet.pdf&usg=AFQjCNGPbKWzv8](https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiM3uGIh6XUAhUEJVAKHQmaBooQFggqMAA&url=http%3A%2F%2Fwww.atmel.com%2FImages%2FAtmel-8495-8-bit-AVR-Microcontrollers-ATtiny441-ATtiny841_Datasheet.pdf&usg=AFQjCNGPbKWzv8).
- [12] ATMEL, «Atmel AT24C01 Datasheet,» [En línea]. Available: <http://www.atmel.com/Images/doc0134.pdf>.



## **12. ANEXOS**



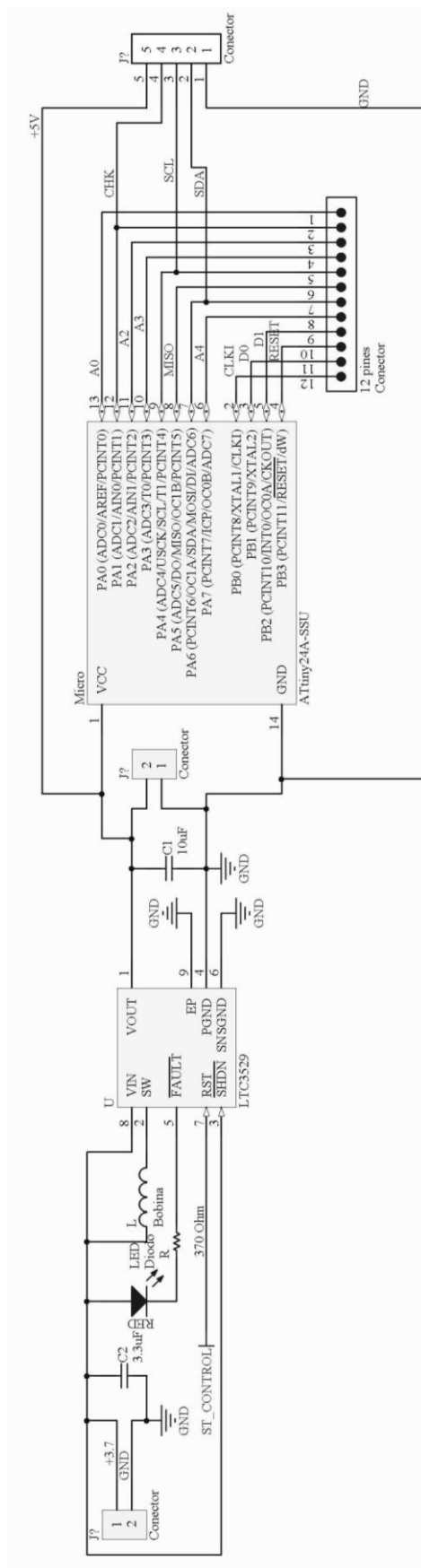
## 12 ANEXOS

### 12.1. Accionamientos

MOTOR				REDUCTOR				
Número de modelo	Potencia (W)	Precio motor	Tensión (V)	Eficiencia %	Par salida (N·mm)	RPM salida	Precio reductor	Precio total
<b>P14356-ND</b>	4,45	3 €	7,4	66	270,6	75	65 €	68 €
<b>P14355-ND</b>	6,50	3 €	5	59	342,2	58	70 €	73 €
<b>P14354-ND</b>	4,37	3 €	5	59	271,4	69	70 €	73 €
<b>P14352-ND</b>	2,75	3 €	3	53	429,3	13	75 €	78 €
<b>P14353-ND</b>	1,65	4 €	3	53	429,3	9	75 €	79 €
<b>P14351-ND</b>	1,40	4 €	3	53	286,2	15	75 €	79 €
<b>MM10</b>	1,23	4 €	3	53	259,9	24	75 €	79 €
<b>MM18</b>	0,51	4 €		53	402,8	9	75 €	79 €
<b>711</b>	-	5 €	6	53	519,8	18	75 €	80 €
<b>MM28</b>	1,64	7 €		53	519,8	19	75 €	82 €
<b>M_3FN</b>	1,80	22 €	6	66	257,4	43	65 €	87 €
<b>M_5FN</b>	1,70	22 €	6	66	264,0	40	65 €	87 €
<b>M_5-BB</b>	4,20	22 €	6	66	290,4	93	65 €	87 €
<b>370C</b>	1,60	17 €	3	59	271,4	33	70 €	87 €
<b>370C</b>	1,30	17 €	6	59	295,0	26	70 €	87 €
<b>RF-500</b>	1,00	17 €	6	59	259,6	22	70 €	87 €
<b>L_5FN</b>	2,30	22 €	2,4	66	290,4	49	65 €	87 €
<b>M_3FN</b>	1,40	22 €	6	59	413,0	19	70 €	92 €
<b>FF-180SH</b>	0,80	17 €	3	53	477,0	8	75 €	92 €
<b>RF-310</b>	0,50	17 €	6	53	381,6	6	75 €	92 €
<b>RF-370</b>	0,50	17 €	6	53	477,0	5	75 €	92 €
<b>RF-500</b>	0,50	17 €	6	53	397,5	6	75 €	92 €
<b>L_3N</b>	0,70	22 €	6	59	330,4	12	70 €	92 €
<b>100044</b>	2,00	62 €	9	59	258,4	62	70 €	132 €
<b>118386</b>	0,75	75 €		53	389,2	21	75 €	150 €
<b>403-1043-ND</b>	13,00	100 €	6	81	320,8	1450	55 €	155 €
<b>323772</b>	90,00	220 €		81	2157,8	532	55 €	275 €

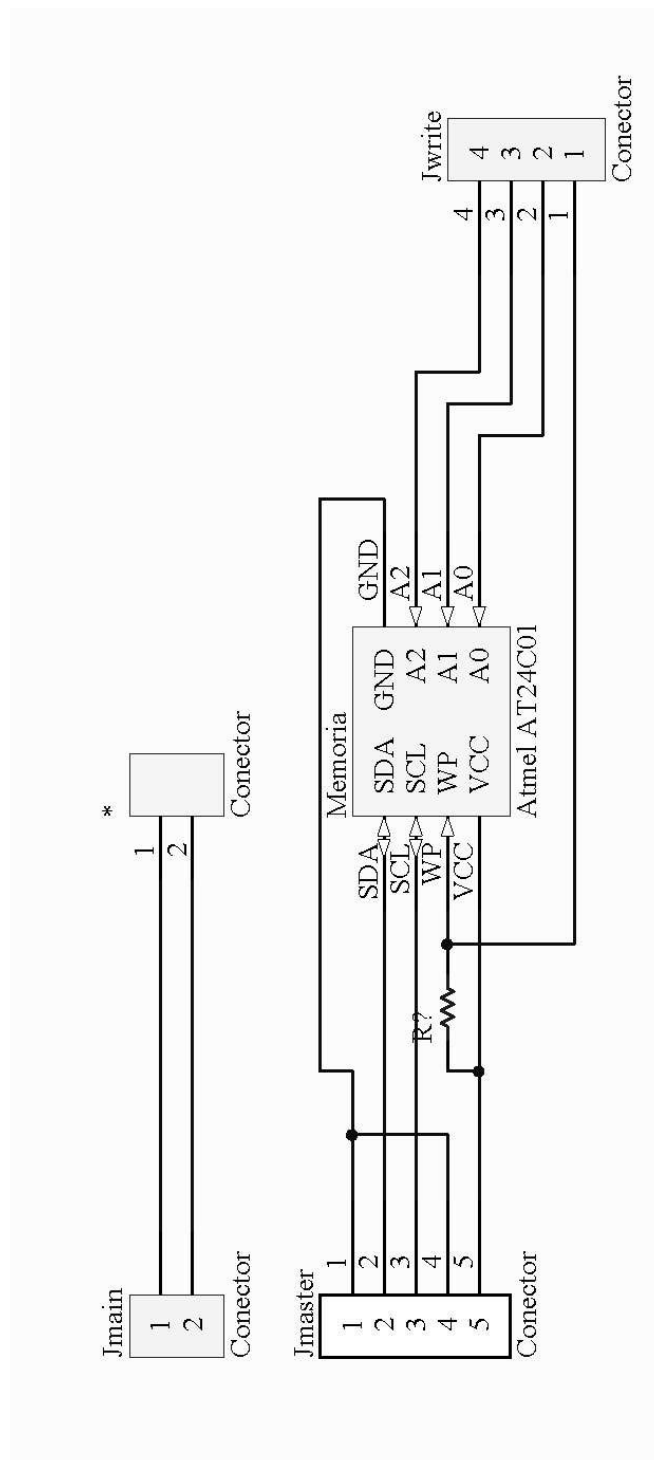
(Fuente: Elaboración propia a partir de datos recopilados de 4 grandes distribuidores de componentes electrónicos: RS online, DigiKey, Farnell y Mouser)

## 12.2. Esquema de conexión placa principal

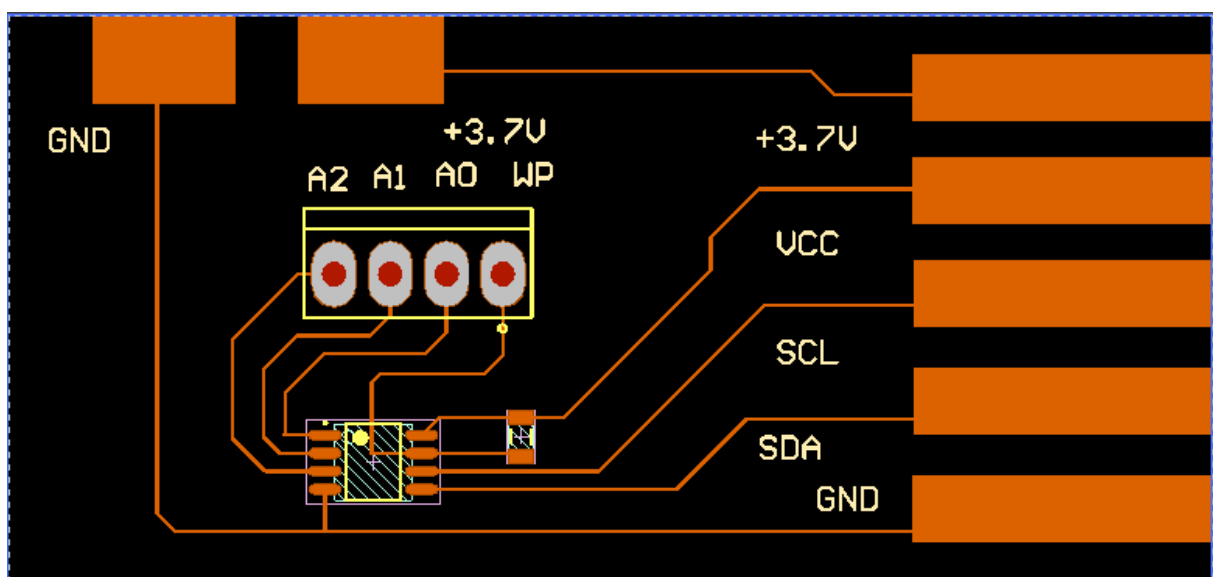
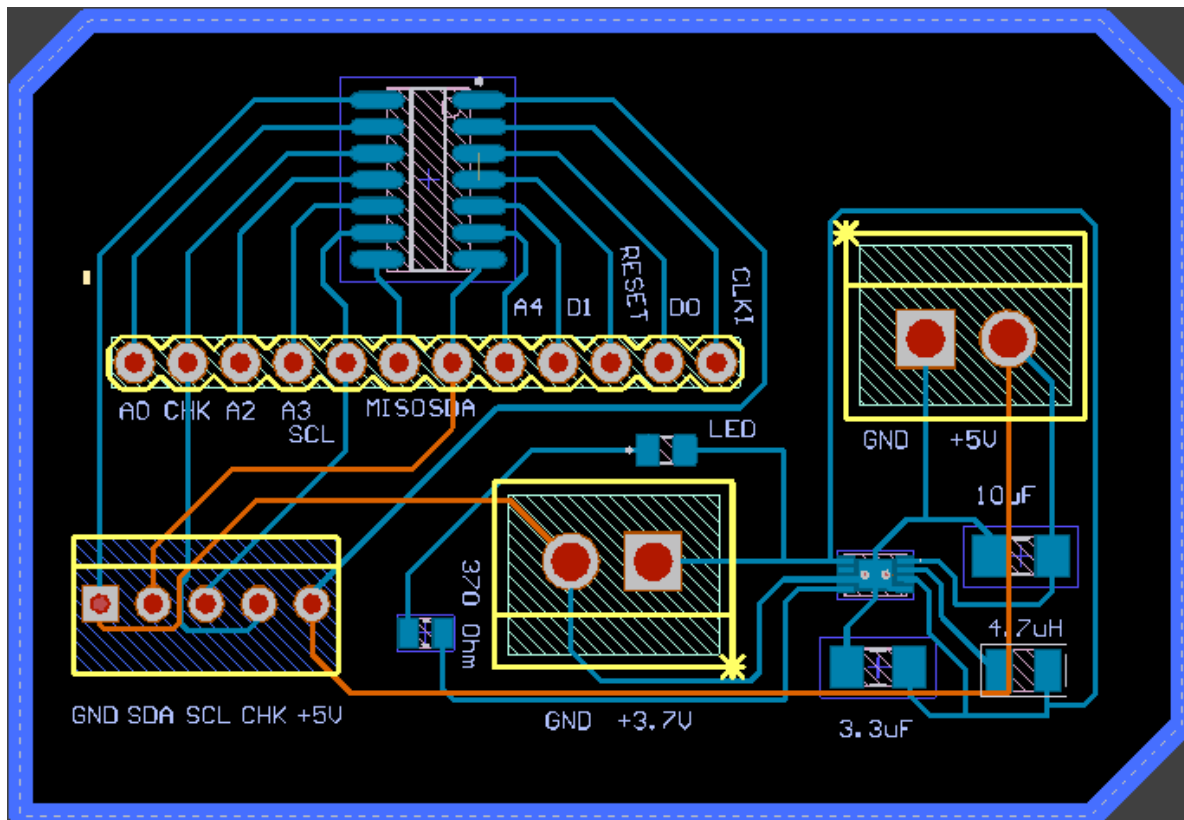




### 12.3. Esquema conexión placa llave



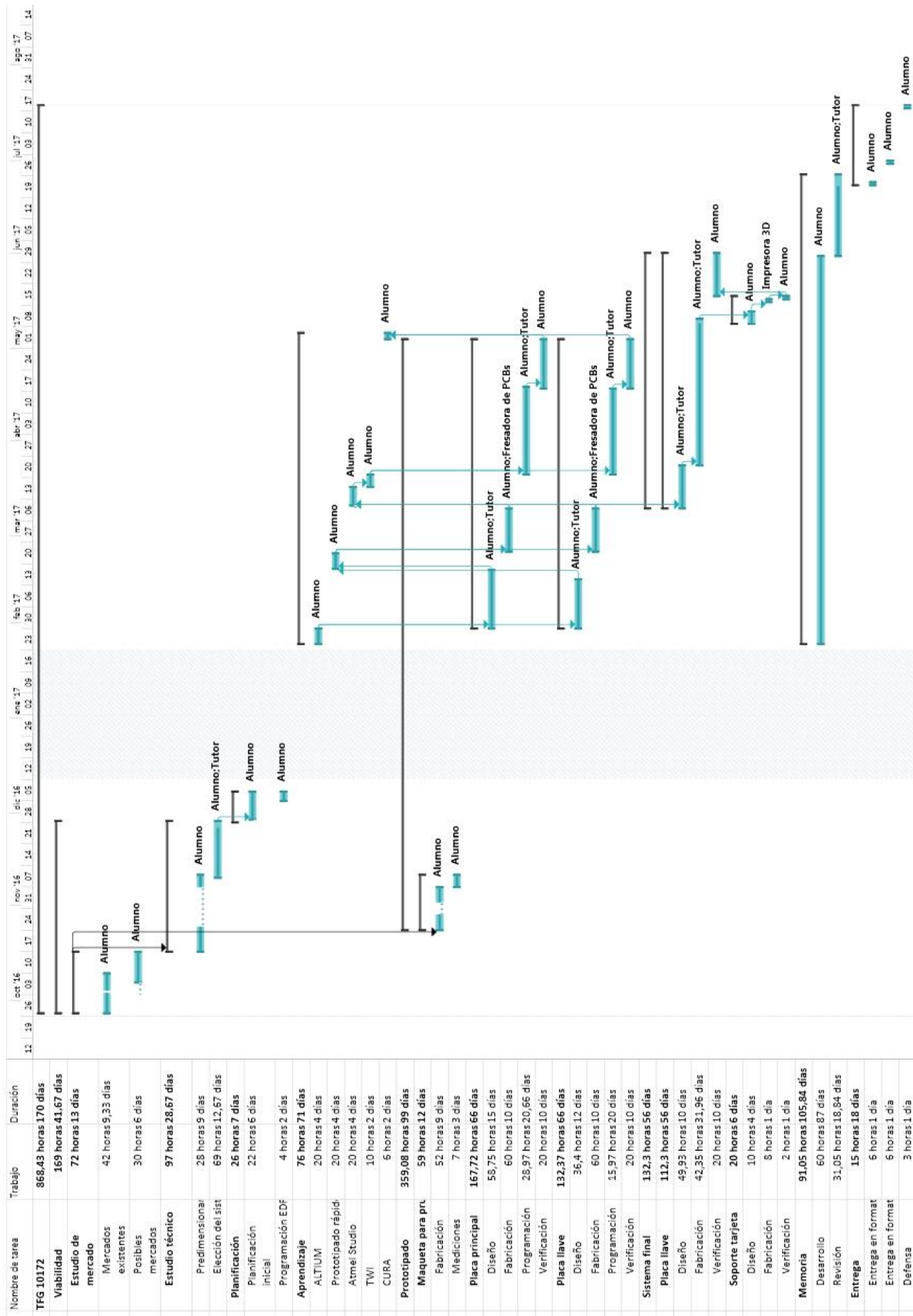
## 12.4. Diseño PCBs



## 12.5. Tareas del proyecto

Nombre	Comienzo	Fin	Trabajo	Costo
TFG 10172	mar 27/09/16	mar 18/07/17	868,43 horas	13.846,57 €
Viabilidad	mar 27/09/16	lun 28/11/16	169 horas	2.755,00 €
Estudio de mercado	mar 27/09/16	dom 16/10/16	72 horas	1.080,00 €
Mercados existentes	mar 27/09/16	dom 09/10/16	42 horas	630,00 €
Posibles mercados	lun 03/10/16	dom 16/10/16	30 horas	450,00 €
Estudio técnico	lun 17/10/16	lun 28/11/16	97 horas	1.675,00 €
Predimensionamiento	lun 17/10/16	jue 10/11/16	28 horas	420,00 €
Elección del sistema	jue 10/11/16	lun 28/11/16	69 horas	1.255,00 €
Planificación	lun 28/11/16	mié 07/12/16	26 horas	390,00 €
Planificación inicial	lun 28/11/16	mié 07/12/16	22 horas	330,00 €
Programación EDP	lun 05/12/16	mié 07/12/16	4 horas	60,00 €
Aprendizaje	mié 25/01/17	vie 05/05/17	76 horas	1.140,00 €
ALTUM	mié 25/01/17	dom 29/01/17	20 horas	300,00 €
Prototipado rápido	sáb 18/02/17	jue 23/02/17	20 horas	300,00 €
Atmel Studio	vie 10/03/17	jue 16/03/17	20 horas	300,00 €
TWI	vie 17/03/17	lun 20/03/17	10 horas	150,00 €
CURA	jue 04/05/17	vie 05/05/17	6 horas	90,00 €
Prototipado	lun 24/10/16	mié 03/05/17	359,08 horas	5.396,37 €
Maqueta para pruebas	lun 24/10/16	jue 10/11/16	59 horas	885,00 €
Fabricación	lun 24/10/16	dom 06/11/16	52 horas	780,00 €
Mediciones	lun 07/11/16	jue 10/11/16	7 horas	105,00 €
Placa principal	lun 30/01/17	mié 03/05/17	167,72 horas	2.615,81 €
Diseño	lun 30/01/17	vie 17/02/17	58,75 horas	981,25 €
Fabricación	vie 24/02/17	jue 09/03/17	60 horas	750,00 €
Programación	mar 21/03/17	mar 18/04/17	28,97 horas	584,56 €
Verificación	mar 18/04/17	mié 03/05/17	20 horas	300,00 €
Placa llave	lun 30/01/17	mié 03/05/17	132,37 horas	1.895,56 €
Diseño	lun 30/01/17	mar 14/02/17	36,4 horas	586,00 €
Fabricación	vie 24/02/17	jue 09/03/17	60 horas	750,00 €
Programación	mar 21/03/17	lun 17/04/17	15,97 horas	259,56 €
Verificación	mar 18/04/17	mié 03/05/17	20 horas	300,00 €
Sistema final	vie 10/03/17	mié 31/05/17	132,3 horas	2.374,41 €
Placa llave	vie 10/03/17	mié 31/05/17	112,3 horas	2.154,41 €
Diseño	vie 10/03/17	jue 23/03/17	49,93 horas	969,12 €
Fabricación	vie 24/03/17	mié 10/05/17	42,35 horas	885,29 €
Verificación	jue 18/05/17	mié 31/05/17	20 horas	300,00 €
Soporte tarjeta	mar 09/05/17	mié 17/05/17	20 horas	220,00 €
Diseño	mar 09/05/17	vie 12/05/17	10 horas	150,00 €
Fabricación	mar 16/05/17	mar 16/05/17	8 horas	40,00 €
Verificación	mié 17/05/17	mié 17/05/17	2 horas	30,00 €
Memoria	mié 25/01/17	lun 26/06/17	91,05 horas	1.565,79 €
Desarrollo	mié 25/01/17	mar 30/05/17	60 horas	900,00 €
Revisión	mié 31/05/17	lun 26/06/17	31,05 horas	665,79 €
Entrega	vie 23/06/17	mar 18/07/17	15 horas	225,00 €
Entrega en formato digital	vie 23/06/17	vie 23/06/17	6 horas	90,00 €
Entrega en formato impreso	vie 30/06/17	vie 30/06/17	6 horas	90,00 €
Defensa	mar 18/07/17	mar 18/07/17	3 horas	45,00 €

## 12.6. Diagrama de Gantt



12.7. Bill Of Materials

Apartado	Nombre	Valor	Vendedor	Ref. Vendedor	Fabricante	Ref. Fabricante	Descripción	Precio unitario	Cantidad mínima	Total
Componentes placa principal	Microprocesador		FARNELL	2396717	ATMEL	Attiny441-SSU	Microprocesador	1,94 €	1	1,94 €
	Diodeo Led	Rojo	FARNELL	1465997	DIALIGHT	5988210107F	Diodeo Led	0,31 €	10	3,10 €
	Condensador	10 uF	MOUSER	77-VJ1206V106ZXQTB8C	Vishay / Vitramon	VJ1206V106ZXQTB8C	Condensador	0,09 €	1	0,09 €
	Condensador	3,3 uF	MOUSER	77-VJ1206V333XXJ8BC	Vishay / Vitramon	VJ1206V333XXJ8BC	Condensador	0,10 €	1	0,10 €
	Resistencia	370 Ohm	MOUSER	660-RN73H1ETP3700D25	KOA Speer	RN73H1ETP3700D25	Resistencia	0,18 €	1	0,18 €
	Bobina	4,7 uH	MOUSER	70-ILSB1206ER4R7K	Vishay / Dale	ILSB1206ER4R7K	Bobina	0,15 €	1	0,15 €
	Conectores jumper		FARNELL				Conectores jumper			0,00 €
	Elevador de tensión		DIGIKEY	LTC3529EDCB#TRMPBFCT-ND	LINEAR TECHNOLOGY	LTC3529	Elevador de tensión	4,46 €	1	4,46 €
Total componentes placa principal:										10,03 €
Componentes placa llave	Memoria EEPROM		FARNELL	556-AT24C01D-STUM-T	ATMEL	AT24C01D-STUM-T	Memoria EEPROM	0,24 €	1	0,24 €
	Resistencia	15k Ohm	MOUSER	71-TNPW080515K08EEA	Vishay	TNPW080515K08EEA	Resistencia	0,67 €	1	0,67 €
	Conector jumper	4 pines	FARNELL				Conector			0,00 €
Total componentes placa llave:										0,91 €
Prototipo definitivo y maqueta	Listones de madera		-	-	-	-	Listones de madera	10,00 €	1	10,00 €
	Servomotor		DIGIKEY	900-00008-ND	Parallax Inc.	900-00008	Servomotor	12,45 €	1	12,45 €
	Cable		Electronica	-	-	-	Cable. Cantidad en metros	0,40 €	2	0,80 €
	Bisagras		-	-	-	-	Bisagras	1,50 €	2	3,00 €
	Cerradura de embutir		Leroy Merlin	15778196	TESA	Embutir 2010	Cerradura de embutir	27,10 €	1	27,10 €
	Batería de litio	2000mAh				504086	Batería de litio		1	0,00 €
	Tornillos						Tornillos	0,15 €	15	2,25 €
Total prototipo definitivo:										55,60 €
Fabricación	SopORTE			Coste estimado según el valor de mercado. Cantidad en horas			SopORTE	5,00 €	4	20,00 €
	Placa principal			Coste estimado según el valor de mercado. Cantidad en horas			Placa principal	10,00 €	1	10,00 €
	Placa llave prototipo			Coste estimado según el valor de mercado. Cantidad en horas			Placa llave prototipo	10,00 €	1	10,00 €
	Placa llave definitiva						Placa llave definitiva			0,00 €
	Maqueta			Coste estimado según el valor de mercado. Cantidad en horas			Maqueta	5,00 €	16	80,00 €
Total fabricación:										120,00 €
TOTAL:										186,536



## ÍNDICE DE FIGURAS

Fig. 1: Sección de un cilindro mecánico de 6 pistones. Se puede apreciar el alineamiento de los pistones que desbloquea el cilindro.....	27
Fig. 2: Cerradura electrónica con formato de cilindro estandarizado .....	29
Fig. 3: Cerradura electrónica con doble sistema de apertura, mecánico y electrónico .....	29
Fig. 4: Cilindro de seguridad con autenticación electrónica .....	30
Fig. 5: Cerradura electrónica “inteligente” con bulón motorizado .....	31
Fig. 6: Cerradura de embutir marca TESA.....	43
Fig. 7: Diagrama de proceso para selección de componentes.....	50
Fig. 8: Diagrama de conexión del componente elevador de tensión LTC3529 .....	54
Fig. 9: Protocolo de comunicación PWM para operar el servomotor en modo de parada.....	59
Fig. 10: Protocolo de comunicación PWM para operar el servomotor a velocidad máxima en sentido horario.....	60
Fig. 11: Protocolo de comunicación PWM para operar el servomotor a velocidad máxima en sentido antihorario.....	60
Fig. 12: Diagrama de conexiones del servomotor elegido .....	61
Fig. 13: Diagrama de bloques del “timer” de 8 bits .....	62
Fig. 14: Diagrama de frecuencias PWM para un valor de comparación constante .....	63
Fig. 15: Diagrama conexiones del sistema.....	68
Fig. 16: Foto de la placa PCB llave definitiva .....	69
Fig. 17: Protocolo de comunicación TWI en microprocesador Atmel. Validación de datos....	70
Fig. 18: Protocolo de comunicación TWI en microprocesador Atmel. Especificación de las condiciones de comienzo y fin de transmisión.....	70
Fig. 19: Protocolo de comunicación TWI en microprocesador Atmel. Bit de comprobación.	71
Fig. 20: Protocolo de comunicación TWI en microprocesador Atmel. Condición de reinicio.	71
Fig. 21: Registro de acceso a la memoria.....	72
Fig. 22: Protocolo de comunicación TWI en microprocesador Atmel. Secuencia de transmisión genérica según el modo de lectura principal (“Current address read”) .....	72
Fig. 23: Protocolo de comunicación TWI en microprocesador Atmel. Secuencia de transmisión genérica según el modo de lectura aleatorio (“Random read”).....	73
Fig. 24: Protocolo de comunicación TWI en microprocesador Atmel. Secuencia de transmisión genérica según el modo de lectura secuencial (“Sequential read”) .....	73
Fig. 25: Fotografía de la placa PCB prototipo. Se pueden distinguir las huellas para soldar la memoria y la resistencia pull-up .....	77
Fig. 26: Fotografía de la tarjeta llave, compuesta por la placa PCB y la batería. Se pueden apreciar los componentes soldados a la placa .....	77
Fig. 27: Imagen renderizada del soporte diseñado en CATIA .....	78
Fig. 28: Fotografía del soporte fabricado mediante impresión 3D y la tarjeta llave.....	78
Fig. 29: Fotografía del soporte fabricado mediante impresión 3D. Se pueden apreciar las tiras de cobre para el contacto con la placa.....	79
Fig. 30: Imagen vectorial del logotipo. Diseñada con Inkscape .....	79
Fig. 31: Fotografía de la placa PCB con la imagen del proyecto. Se puede leer “SPS – Self-Powered Smart Lock” .....	80
Fig. 32: EDP del proyecto .....	93
Fig. 33: Diagrama de Gantt resumen .....	94





## ÍNDICE DE TABLAS

Tabla 1: Valores medido de par de apertura de una cerradura instalada en una puerta doméstica convencional. ....	40
Tabla 2: Comparativa procesadores bajo consumo de la marca Atmel.....	51
Tabla 3: Comparativa memorias flash de bajo consumo de la marca Atmel .....	52
Tabla 4: Comparativa elevadores de tensión.....	54
Tabla 5: Especificaciones de tensión para el correcto funcionamiento del servomotor.....	59
Tabla 6: Dirección de los registros TOCC .....	61
Tabla 7: Especificación de los registros COMnAx y COMnBx con modo “Fast PWM” activado .....	62
Tabla 8: Tabla de valores de pico (TOP) en función de la velocidad de giro deseada (izquierda) y tabla de especificaciones necesarias para el cálculo de dichos valores (derecha) .....	64
Tabla 9: Fases del proyecto y coste real desglosado para cada fase.....	94
Tabla 10: Recursos del proyecto y coste de los mismos .....	95
Tabla 11: Abreviaturas y acrónimos .....	117
Tabla 12: Unidades utilizadas .....	118
Tabla 13: Prefijos del sistema internacional.....	118



## ÍNDICE DE CUADROS

Cuadro 1: Código de llamada a la librería para la comunicación TWI mediante software .....	74
Cuadro 2: Modificación de los registros para el acceso a la memoria .....	74
Cuadro 3: Función de la librería TWI para la lectura de un byte .....	75
Cuadro 4: Función de la librería TWI encargada de iniciar el protocolo de comunicación.....	75
Cuadro 5: Función de la librería TWI encargada de leer el dato recibido de la memoria.....	76
Cuadro 6: Función de la librería TWI encargada de detener la comunicación. ....	76



## ABREVIATURAS, UNIDADES Y ACRÓNIMOS

### Abreviaturas y Acrónimos

Abreviatura	Definición
<b>DIY</b>	<b>Do It Yourself</b> Hágalo usted mismo
<b>PWM</b>	<b>Pulse-Width Modulation</b> Modulación por ancho de pulso
<b>I2C</b>	<b>Inter-Integrated Circuit</b> Circuitos interintegrados
<b>TWI</b>	<b>Two Wire Interface</b> Interfaz de dos hilos
<b>SPI</b>	<b>Serial Peripheral Interface</b> Interfaz periférica en serie
<b>BOM</b>	<b>Bill Of Materials</b> Lista de materiales
<b>RFID</b>	<b>Radio-Frequency IDentification</b> Indentificación por radiofrecuencia
<b>NFC</b>	<b>Near Field Communication</b> Comunicación por campo cercano
<b>PCB</b>	<b>Printed Circuit Board</b> Placa de circuito impreso
<b>SDA</b>	<b>Serial DATA line</b> Linea de datos en serie
<b>SCL</b>	<b>Serial Clock Line</b> Linea de reloj en serie
<b>GND</b>	<b>Ground</b> Tierra
<b>QR</b>	<b>Quick-Response</b> Respuesta rápida
<b>ADN</b>	<b>Ácido Desoxirribonucleico</b>

*Tabla 11: Abreviaturas y acrónimos*  
(Fuente: Recopilación del documento)

**Unidades**

Unidades	Definición
<b>V</b>	Voltios Tensión eléctrica
<b>A</b>	Amperios Corriente eléctrica
<b>N</b>	Newton Fuerza
<b>J</b>	Julios Energía
<b>W</b>	Vatios Potencia
<b>H</b>	Henrios Inductancia eléctrica
<b>m</b>	Metros Distancia
<b>RPM</b>	Revoluciones por minuto Velocidad de giro
<b>s</b>	Segundos Tiempo

*Tabla 12: Unidades utilizadas*  
(Fuente: Recopilación del documento)

**Prefijos del sistema internacional**

deci (d)	$10^{-1}$	deca (da)	$10^1$
centi (c)	$10^{-2}$	hecto (h)	$10^2$
mili (m)	$10^{-3}$	kilo (k)	$10^3$
micro (μ)	$10^{-4}$	mega(M)	$10^4$
nano (n)	$10^{-5}$	giga (G)	$10^5$
pico (p)	$10^{-6}$	tera (T)	$10^6$

*Tabla 13: Prefijos del sistema internacional*  
(Fuente: [www.bipm.org](http://www.bipm.org))

|





## **GLOSARIO**

### **Bombín**

También llamado cilindro o bombillo. Es la pieza donde se inserta la llave (en las cerraduras con bombín, que no son todas) y que aloja el mecanismo que decide qué llaves accionan la cerradura. Esta pieza se puede cambiar independientemente del resto de la cerradura.

### **Control de acceso**

El control de acceso consiste en la verificación de si una entidad (una persona, vehículo, ordenador, etc.) solicitando acceso a un recurso tiene los derechos necesarios para hacerlo.

Un control de acceso ofrece la posibilidad de acceder a recursos físicos (por ejemplo, a un edificio, a un local, a un país) o lógicos (por ejemplo, a un sistema operativo o a una aplicación informática específica). [11]

### **Autenticación**

La autenticación es el acto o proceso de confirmar que algo (o alguien) es quien dice ser. A la parte que se identifica se le llama probador, mientras que se denomina verificador a la parte que verifica la identidad. Es habitual que el probador sea un usuario que quiere acceder a ciertos recursos y el verificador sea un sistema que protege el acceso a aquellos, comprobando que el que accede sea un usuario que tiene permisos para ello.

### **Resbalón**

La pieza que se retrae dentro de la caja al accionar la manilla y que mantiene la puerta cerrada mientras la llave no se ha echado. Tiene un lado en forma de cuña para permitir el deslizamiento de la puerta.

### **Paletón/bulones**

Son las piezas que se retraen dentro de la puerta pero, en este caso, mediante llave, a diferencia del resbalón que es mediante un resorte. Por tanto, al cerrar la puerta con llave salen y se introducen en el marco, imposibilitando la apertura.

La diferencia entre ambos radica en la forma geométrica, siendo el paletón una pieza cubica, de lados paralelos, y los bulones piezas cilíndricas.

### **RFID**

RFID son las siglas de Radio Frequency Identification, (en español identificación por radiofrecuencia), es un método de almacenamiento y recuperación de datos que usa dispositivos

como tarjetas o tags RFID. Un sistema RFID está basado en los siguientes elementos: transponder o tag, lector y software.

### **Ganzuado**

Referido a la acción de emplear una ganzúa para abrir una cerradura. Este proceso consiste en el levantamiento de los pines de la cerradura uno a uno hasta que quede completamente desbloqueada.

### **Bumping**

Técnica para abrir cerraduras sin forzarlas. Desarrollada en la década de 1970 por algunos cerrajeros en Dinamarca, con el fin de desbloquear los cilindros de una cerradura. La técnica consistía en presionar ligeramente una llave especialmente diseñada, llave *bumping*, con un objeto, haciendo saltar los cilindros. Esto provocaba que la cerradura pudiera deslizarse libremente, permitiendo así el desbloqueo del cilindro.

### **Extractor**

Herramienta diseñada para la extracción de cerraduras de cilindro desde el exterior. Se trata de una herramienta levemente destructiva, pues rompe el cilindro por el punto de anclaje a la puerta y permite extraerlo para la posterior apertura mediante una llave de leva.

### **SMART TV**

La televisión inteligente (en inglés, smart TV) es la integración de internet y de las características Web 2.0 a la televisión digital (en especial, a la televisión 3D) y al set-top box (STB), así como la convergencia tecnológica entre los ordenadores y estos televisores y el STB.

### **NFC**

El NFC (Near Field Communication) es una tecnología inalámbrica de corto alcance que permite conectar dos dispositivos al emitir una señal, y que al mismo tiempo puede también recibir una señal. Permite, por lo tanto, una lectura-escritura en ambos sentidos.

### **WiFi**

El Wifi o Wi-Fi es una marca comercial de la empresa Wi-Fi Alliance la cual es una organización que certifica y es propietaria del standard 802.11 de redes inalámbricas de área local. El Wifi sirve para conectar a diferentes equipos a la red de manera inalámbrica. Esta conexión es compatible con casi todos los equipos que tengan un receptor de ondas inalámbricas de Wifi.

## **BLUETOOTH**

Bluetooth es una especificación tecnológica para redes inalámbricas que permite la transmisión de voz y datos entre distintos dispositivos en una frecuencia determinada (2,4 GHz).

## **Servomotor**

Un servomotor (también llamado servo) es un dispositivo similar a un motor de corriente continua que tiene la capacidad de ubicarse en cualquier posición dentro de su rango de operación y, mantenerse estable en dicha posición.

## **PWM**

La modulación por ancho de pulsos (también conocida como PWM, siglas en inglés de pulse-width modulation) de una señal o fuente de energía es una técnica en la que se modifica el ciclo de trabajo de una señal periódica (una senoidal o una cuadrada, por ejemplo), ya sea para transmitir información a través de un canal de comunicaciones o para controlar la cantidad de energía que se envía a una carga.

## **PCB**

Una placa de circuito impreso (del inglés: Printed Circuit Board, PCB), es la superficie constituida por caminos, pistas o buses de material conductor laminadas sobre una base no conductora. El circuito impreso se utiliza para conectar eléctricamente a través de las pistas conductoras, y sostener mecánicamente, por medio de la base, un conjunto de componentes electrónicos.

## **Convertidor Boost**

El convertidor Boost (o elevador) es un convertidor DC a DC que obtiene a su salida una tensión continua mayor que a su entrada. Es un tipo de fuente de alimentación conmutada que contiene al menos dos interruptores semiconductores (diodo y transistor), y al menos un elemento para almacenar energía (condensador, bobina o combinación de ambos).

## **Timer**

Temporizador en inglés. En microcontroladores se emplea este término para referirse a un registro que aumenta su valor en una unidad con cada ciclo de reloj al cual se encuentre funcionando el microcontrolador.

## **Registro**

Son un espacio de memoria muy reducido pero necesario para cualquier microprocesador. De

aquí se toman los datos para varias operaciones que debe realizar el resto de los circuitos del procesador. Los registros sirven para almacenar los resultados de la ejecución de instrucciones, cargar datos desde la memoria externa o almacenarlos en ella.

### **I2C**

Un circuito interintegrado (I<sup>2</sup>C, del inglés Inter-Integrated Circuit) es un bus serie de datos desarrollado en 1982 por Philips Semiconductors. Se utiliza principalmente internamente para la comunicación entre diferentes partes de un circuito, por ejemplo, entre un controlador y circuitos periféricos integrados.

### **TWI**

Término introducido por Atmel para referirse al protocolo I2C, dado que dicho protocolo estaba protegido por una patente. Desde el punto de vista técnico, TWI e I<sup>2</sup>C son idénticos. Sin embargo, el 1 de octubre 2006, la patente original caducó, así que ya no hay derechos de autor para el uso del término I<sup>2</sup>C. I<sup>2</sup>C no es tampoco una marca comercial registrada de NXP Semiconductors, la protección de marca es sólo para el logotipo.

### **SDA**

Línea de datos empleada por el protocolo I2C (Serial Data en inglés).

### **SCL**

Línea de reloj empleada por el protocolo I2C. El nombre deriva de las iniciales de “Serial Clock Line”.

### **GND**

Proviene del inglés, “Ground”. Nombre abreviado para referirse al valor de base de tensión en el circuito electrónico, denominado “tierra”.

### **VCC**

Nombre abreviado para referirse al valor de tensión positiva de funcionamiento en el circuito electrónico.

### **Código abierto**

El código abierto es el software desarrollado y distribuido libremente. Se focaliza más en los beneficios prácticos (acceso al código fuente) que en cuestiones éticas o de libertad que tanto se destacan en el software libre. Para muchos el término «libre» hace referencia al hecho de adquirir un software de manera gratuita, pero más que eso, la libertad se refiere al poder

modificar la fuente del programa sin restricciones de licencia, ya que muchas empresas de software encierran su código, ocultándolo, y restringiéndose los derechos a sí misma.

## **Vectorial**

Una imagen vectorial es una imagen digital formada por objetos geométricos dependientes (segmentos, polígonos, arcos, muros, etc.), cada uno de ellos definido por atributos matemáticos de forma, de posición, etc. Por ejemplo un círculo de color rojo quedaría definido por la posición de su centro, su radio, el grosor de línea y su color.

## **Códigos QR**

Un código QR es la evolución del código de barras. Es un módulo para almacenar información en una matriz de puntos o en un código de barras bidimensional.

## **Biometría**

La biometría es la toma de medidas estandarizadas de los seres vivos o de procesos biológicos. La “autenticación biométrica” o “biometría informática” es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para su autenticación, es decir, verificar su identidad.

Las huellas dactilares, la retina, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas estáticas, mientras que entre los ejemplos de características dinámicas se incluye la firma, el paso o la manera de teclear. Algunos rasgos biométricos, como la voz, comparten aspectos físicos y del comportamiento.

## **ADN**

El ácido desoxirribonucleico, abreviado como ADN, es un ácido nucleico que contiene las instrucciones genéticas usadas en el desarrollo y funcionamiento de todos los organismos vivos conocidos y algunos virus, y es responsable de su transmisión hereditaria. La función principal de la molécula de ADN es el almacenamiento a largo plazo de información.

El ADN es único para cada ser vivo, por lo que puede utilizarse como característica estática en la autenticación biométrica.

## **Reconocimiento facial**

El sistema de reconocimiento facial es una aplicación dirigida por un ordenador que identifica automáticamente a una persona en una imagen digital. Esto es posible mediante un análisis de las características faciales del sujeto extraídas de la imagen o de un fotograma clave de una

fuentes de video, y comparándolas con una base de datos.

### **Ad-hoc**

Generalmente se refiere a una solución específicamente elaborada para un problema o fin preciso y, por tanto, no generalizable ni utilizable para otros propósitos.

Se usa pues para referirse a algo que es adecuado sólo para un determinado fin o en una determinada situación.

### **Red centralizada**

Sistema diseñado para traspasar la información (o las ordenes) desde un único punto. Un ejemplo clásico sería el de la televisión. La información se emite desde un único punto y los receptores (las antenas de televisión repartidas por el territorio) reciben la información que quieren dar desde ese punto central.

### **Red descentralizada**

En este sistema no existe un único nodo central, sino un centro colectivo de conectores. La caída de uno de los nodos centralizadores conlleva la desconexión de uno o más nodos del conjunto de la red mientras que la caída del cluster centralizador produciría necesariamente la ruptura y práctica desaparición de la red.

### **Red distribuida**

Con este sistema la extracción de cualquiera de los nodos no desconectaría de la red a ningún otro. Todos los nodos se conectan entre sí sin que tengan que pasar necesariamente por uno o varios centros locales. En este tipo de redes desaparece la división centro periferia y por tanto el poder de filtro sobre la información que fluye por ella.

### **Blockchain**

Una cadena de bloques, también conocida por las siglas BC (del inglés Blockchain) es una base de datos distribuida, formada por cadenas de bloques diseñadas para evitar su modificación una vez que un dato ha sido publicado usando un sellado de tiempo confiable y enlazando a un bloque anterior. Por esta razón, es especialmente adecuada para almacenar datos ordenados de forma creciente en el tiempo y sin posibilidad de modificación ni revisión.









**POLITÉCNICA**

**ESCUELA TÉCNICA SUPERIOR DE INGENIEROS INDUSTRIALES  
UNIVERSIDAD POLITÉCNICA DE MADRID**

José Gutiérrez Abascal, 2, 28006 Madrid

Tel.: 91 336 3060

[info.industriales@upm.es](mailto:info.industriales@upm.es)

[www.industriales.upm.es](http://www.industriales.upm.es)